MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE

SCIENTIFIQUE ET DE L'INNOVATION

ECOLE SUPERIEURE DE COMMERCE ET D'INFORMATIQUE DE GESTION (ESCO-IGES)

BURKINA FASO

UNITE-PROGRES-JUSTICE

MTOPO PAYMENT SOLUTIONS BF

MEMOIRE DE FIN DE CYCLE

Stage éffectué du 22 mai 2018 au 21 octrobre 2018

Présenté en vue d'obtention du diplome de master 2 professionel

Domaine:Droit des Affaires et Fiscalité

THEME :

PROTECTION DES DONNEES D'UTILISATEURS A CARACTERE PERSONNEL SUR LES PROGRAMMES D'ORDINATEURS AU BURKINA FASO : CAS DE MTOPO PAYMENT SOLUTIONS BF,TSR ET RAHIMO TRANSPORT.

Présenté par : ***Hamidou SOUDRE***

Directeur de mémoire :

Anatole KABORE

Magistrat, enseignant vacataire

Maitre de stage :

Seny GANEMTORE

Directeur Général de MTOPO

Année académique : 2017-2018

AVERTISSEMENT

L'Ecole Supérieure de Commerce et d'Informatique de Gestion n'entend donner aucune approbation ou improbation au contenu du document. Les idées émises n'engagent que leur auteur.

DEDICACE

A mon cher père, qui a toujours cru en moi et a mis à ma disposition tous les moyens nécessaires pour que je réussisse dans mes études. A ma chère mère, que je ne cesse de remercier pour tout ce qu'elle m'a donné. Que Dieu la récompense pour tous ses bienfaits. A mes amis pour la solidarité et le partage.

REMERCIEMENTS

Au terme de notre étude, nous exprimons notre profonde reconnaissance à notre directeur de mémoire, Monsieur Anatole KABORE, qui n'a ménagé aucun effort pour nous apporter ses précieux conseils, ses encouragements et ses suggestions. Nous tenons, en outre, à remercier nos enseignants et l'ensemble du personnel de ESCO IGES pour avoir assuré notre formation tout en nous donnant des conseils pour une meilleure intégration dans la fonction publique et dans le monde des affaires. Nos remerciements s'adressent également à toute l'administration de MTOPO PAYEMENT SOLUTIONS BF, en particulier notre directeur de stage, Monsieur Seny GANEMTORE et à toute l'administration de TSR et RAHIMO Transport. Nous remercions par ailleurs nos proches, nos camarades et nos amis pour leurs différents soutiens et encouragements qui nous ont permis de mener notre étude. Nous remercions, enfin, tous ceux qui, de près ou de loin, et de quelque manière que ce soit nous ont été utiles dans la réalisation de ce mémoire.

LISTE DES SIGLES, ABREVIATIONS ET ACRONYMES

AN	**A**ssemblée **N**ationale
BF	**B**urkina **F**aso
CE	**C**onseil **E**uropéen
CE	**C**onseil de l'Europe
CEDEAO	**C**omité **E**conomique Des **E**tats de l'**A**frique de l'**O**uest
CEDH	**C**onvention **E**uropéenne des **D**roits de l'**H**omme
CENI	**C**ommission **E**lectorale **N**ationale **I**ndépendante
CIL	**C**ommission de l'**I**nformatique et des **L**ibertés
CNIL	**C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés
CNSS	**C**aisse **N**ationale de la **S**écurité **S**ociale
CUA	**C**onvention de l'Union Africaine
DAAF	**D**irection des **A**ffaires **A**dministratives et **F**inancières
DAJC	**D**irection des **A**ffaires **J**uridiques et du **C**ontentieux
DETC	**D**irection de l'**E**xpertise **T**echnique et du **C**ontrôle
DF	**D**épartement **F**inance
DG	**D**irection **G**énérale
DTIC	**D**roit des **T**echnologies de l'**I**nformatique et de la **C**ommunication
DUDH	**D**éclaration **U**niverselle des **D**roits de l'**H**omme
ESCO-IGES	**E**cole de **C**ommerce et d'**I**nformatique de **G**estion
GAFAM	**G**oogle **A**mazon **F**acebook **A**pple **M**icrosoft
GDRP	**G**eneral **D**ata **R**egulation and **P**rotection
JO	**J**ournal **O**fficiel
LIL	**L**oi **I**nformatique et **L**ibertés
LPDP	**L**oi portant **P**rotection des **D**onnées à caractère **P**ersonnel
NTIC	**N**ouvelles **T**echnologies de l'**I**nformation et de la **C**ommunication
OIF	**O**rganisation **I**nternationale de la **F**rancophonie
ONI	**O**ffice **N**ationale d'**I**dentification
ONU	**O**rganisation des **N**ations **U**nies
PIN	**P**ersonal **I**dentification **N**umber
SAS	**S**oftware **A**s a **S**ervice
SG	**S**ecrétariat **G**énéral
SRHJ	**S**ervice des Ressources Humaines et Juridiques

TSR	**T**ransport **S**ana **R**asmané
UA	**U**nion **A**fricaine
UE	**U**nion **E**uropéenne
UNESCO	**O**rganisation des **N**ations **U**nies pour l'**E**ducation, la **S**cience et la **C**ulture
USA	**U**nited **S**tate of **A**merica

LISTE DES TABLEAUX.

SOMMAIRE

AVANT -PROPOS

L'Ecole Supérieure de Commerce et d'Informatique de Gestion (ESCO-IGES) est un établissement privé d'enseignement supérieur qui a ouvert ses portes en octobre de l'année académique 1999-2000 par décret n°2000/444/MESSRS du 13 mai 2000.L'école est en partenariat depuis 2003 avec la Fondation Université Mercure (FUM) de Bruxelles en Belgique, l'Etat burkinabè et l'Institut Burkinabé des Arts et Métiers (IBAM) de l'université Joseph Ki Zerbo.

L'école forme des agents de maitrises, des cadres moyens et des cadres supérieurs dans les filières suivantes :

- **Premier cycle**
- DTS ou BTS Banque ;
- DTS ou BTS Finance Comptabilité ;
- DTS ou BTS Gestion Commerciale ;
- DTS ou BTS Communication d'entreprise ;
- DTS ou BTS Transport Logistique et Transit ;
- DTS ou BTS Marketing Management.

- **Second Cycle**
- Licence Professionnelle en Technique Comptable et Financière ;
- Licence Professionnelle en Gestion des Ressources Humaines ;
- Licence Professionnelle en Marketing et Communication d'entreprise ;
- Maitrise en Gestion des Ressources Humaines ;
- Maitrise en Sciences et Techniques Comptables et Financières ;
- Maitrise en marketing Vente ;
- Maitrise en Informatique ;
- Master Professionnel en Droit des Affaires et Fiscalités ;
- Master en Management des Ressources Humaines ;
- Master Professionnel en Management des affaires.

C'est le second cycle qui nous concerne et plus précisément le Master en Droit des Affaires et Fiscalité.

A la fin de ce cycle théorique, l'étudiant doit produire un mémoire pour l'obtention de son diplôme de master II. Pour ce faire, nous avons décidé d'effectuer un stage dans une société commerciale. Le thème retenu est : « Protection des données d'utilisateurs à caractère personnel sur les programmes d'ordinateurs au Burkina Faso : cas de MTOPO PAYMENT SOLUTIONS BF, TSR et RAHIMO TRANSPORT ».

INTRODUCTION GENERALE

Avec la multiplication des dispositifs de mise en relation ainsi que le développement des applications participatives sur l'internet[1], la question de la protection des données personnelles a émergé parallèlement avec la question de l'exploitation marchande de ces données par les entreprises de l'internet[2] entrainant ainsi la menace de la vie privée des utilisateurs. Cette question est relativement récente au regard de l'évolution de l'internet. Elle ne se posait pas de façon aussi sensible lors des débuts de Google en 1998 ou de Facebook en 2004[3], car la marchandisation de ces données n'était pas autant au cœur des services proposés par ces deux entreprises. Pour percevoir l'intensité de ces progrès et des bouleversements qui en découlent, il suffit de réaliser que, pendant cette période, les progrès scientifiques et technologiques ont permis de multiplier par mille la vitesse de traitement de l'information, les capacités de stockage et les capacités de communication[4].Avec l'avancée technologique de l'informatique et les multiples possibilités économiques qui en découlent, cette question de la protection des données personnelles devient centrale et suscite de nombreux débats juridiques, techniques, économiques et sociologiques. De ce fait, ces dernières années, le droit à la vie privée[5] s'est vu de plus en plus menacé par le développement exponentiel des nouveaux systèmes d'information et de collecte des données personnelles.

Aucun pays du monde n'arrive à protéger de façon efficace les données personnelles de ses citoyens. Ce qui signifie qu'il n'existe aucun pays qui puisse veiller à la protection effective de la vie privée de sa population face à ces divers facteurs de risques.

Pourtant, ce phénomène est en contradiction avec les instruments nationaux et internationaux en matière de protection de la vie privée et des données personnelles. Afin d'éradiquer de telles situations, les Etats ont mis en place des règles juridiques spécifiques en matière de protection des données à caractère personnel de leurs citoyens.

---

[1] L'internet est un réseau informatique mondial accessible au public. Il peut être aussi définit comme un réseau mondial de télécommunication reliant entre eux des ordinateurs ou des réseaux locaux et permettant l'acheminement des données numérisées de toutes sortes (messages électroniques, images, textes, sons, ct.), in www.kalieu-elongo.com/reseaux-sociaux ,consulté le 02/05/2019 à 11h.

[2] N. WALCZAK, protection des données personnelles sur l'internet, France, ed.2014, 04 juillet 2014, p.14, in https://halshs.archives-ouvertes.fr/tel-01271019/document consulté le (01/01/2019 à 14h)

[3]Ce que nous avons constaté dans l'élaboration de notre mémoire. Avant cette date, les données personnelles ne constituaient pas des enjeux économiques et politiques pour les entreprises de technologie, ce qui est, le cas, dans l'actualité et à partir de 2008.

[4] G. BRAIBANT, Données personnelles et société de l'information, Rapport au Premier Ministre français sur la transposition en droit français de la directive n° 95/46, documentation française, le 03 mars 1998, p.1.

[5] E. DECAUX, Professeur d'université Paris II, « Protection de la vie privée au regard des données informatiques », article, 2003, p.1.in http//www.enssib.fr.document.123…PDF.

Le Burkina Faso en tant que pays en voie de développement ne déroge pas à cette règle.

Les différents référentiels de protection des données à caractère personnel adoptés par les autorités accordent une place non négligeable à la protection décente de la vie privée de la population. Toutefois, on peut regretter que la protection décente des données personnelles reste encore une préoccupation pour la population. Il faut rechercher des voies et moyens pour sortir de cette impasse afin que toute la population dont les données personnelles font l'objet de traitement par les responsables des traitements puisse être utilisée conformément à la loi n° 010 du 20 avril 2004 portant protection des données à caractère personnel au Burkina Faso.

L'un des moyens pour y parvenir est l'information des citoyens de la finalité des traitements des données à caractère personnel par l'entremise de plusieurs moyens jugés appropriés. Ainsi, l'individu acquiert des moyens lui permettant de réguler lui-même ses données personnelles à travers l'exercice des contrôles, à posteriori, de la mise en œuvre de traitement des données à caractère personnel.

C'est d'ailleurs l'objectif assigné par la loi n° 010 du 24 avril 2004 portant protection des données à caractère personnel au Burkina Faso[6]. L'article 13 de cette loi dispose que le responsable des traitements des données à caractère personnel est dans l'obligation « *d'informer les personnes concernées de la finalité du traitement, des destinataires des données…* »[7] L'information des personnes concernées joue un rôle très important dans la mesure où elle a pour vocation de permettre aux personnes concernées d'auto-protéger leur vie privée.

Le marché burkinabè est confronté à de nouveaux enjeux commerciaux à l'ère du numérique dans le secteur de transport terrestre de personnes qui utilise des logiciels de gestion de leurs activités[8]. Le développement exponentiel des technologies de l'information et de la communication interpelle en ce qu'il entraine une intrusion massive dans la vie privée des citoyens,[9] des consommateurs[10]. Ces innovations favorisent l'extraction de ce que l'on nomme aujourd'hui le nouvel or noir du 21ème siècle : les données personnelles, nouvel eldorado des grandes entreprises.

---

[6] La loi n°010 du 24 avril 2004 est la première législation burkinabè en matière de protection des données à caractère personnel au Burkina Faso. Le Burkina Faso fut le premier pays à adopter une législation en matière de protection des données personnel en Afrique.

[7] Article 13 de la loi n°010 du 20 Avril 2004 portant protection des données à caractère personnel au Burkina Faso.

[8] Nous avons constaté lors de notre voyage Ouaga-Bobo en Mai 2018 que les compagnies de transport terrestre de personnes, en particulier, Transport Sana Rasmané et RAHIMO TRANSPORT évoluent dans les technologies. Elles utilisent un logiciel de vente des tickets de transport qui collecte des données nominatives et les numéros du téléphone de leurs clients.

[9] L.Marie, Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique, France, HAL, ed.2018, p.8.

[10] Définie comme « toute personne physique agissant à des fins qui n'entrent pas dans le cadre de son activité professionnelle » article 2 alinéa 5 loi n° 045-2009/an portant règlementation des services et des transactions électroniques au Burkina Faso. JO n°01 du 07 janvier 2010.

Dans cet environnement, les données à caractère personnel des personnes concernées sur les logiciels ne sont-elles pas détournées de leur finalité ? En d'autres termes, les données personnelles des personnes concernées sur les logiciels ne sont-elles pas utilisées à d'autres finalités autres que celles pour laquelle elles ont été collectées ?

Pour apporter une réponse à cette problématique, nous avons opté d'étudier la protection des données à caractère personnel à travers le cas spécifique de MTOPO PAYEMENT SOLUTIONS BF, TSR et RAHIMO TRANSPORT.

Nous examinerons la problématique posée en scindant notre travail en deux parties distinctes. La première partie sera consacrée au cadre théorique de l'étude analytique et les conditions d'utilisation des données à caractère personnel au Burkina Faso. La deuxième partie se focalisera sur l'analyse et l'interprétation des résultats et les propositions de solutions pour une meilleure amélioration de la protection de la vie privée de la population en général et en particulier des usagers des compagnies de transport TSR et RAHIMO TRANSPORT.

PREMIERE PARTIE : CADRE THEORIQUE, METHODOLOGIQUE ET CONDITIONS D'UTILISATIONS DES DONNEES A CARACTERE PERSONNEL AU BURKINA FASO

Cette partie comporte deux (02) chapitres. Le premier chapitre traite du cadre théorique et méthodologique de l'étude et le deuxième chapitre est réservé aux conditions d'utilisations des données à caractère personnel au Burkina Faso.

Chapitre I : Cadre théorique et méthodologique de l'étude.

Pour les besoins de la présente étude, il nous a fallu élaborer un cadre théorique (section I) et méthodologique (section II).

Section I : Cadre théorique de l'étude

Le cadre théorique de l'étude pose, d'abord, la problématique, la justification, les objectifs et les questions de recherche (paragraphe I). Il est axé sur l'intérêt, les hypothèses de recherche et le cadre conceptuel (paragraphe II).

Paragraphe I : La problématique, la justification, les objectifs et les questions de recherche

Il convient de poser, d'abord, la problématique et la justification du choix du thème(A), puis les objectifs et les questions de recherche(B).

A. La problématique et la justification

Cette rubrique traite du problème que pose le thème (1) et donne ensuite la justification du choix de ce thème (2).

1. La problématique

La protection de la vie privée[11] des personnes physiques demeure une préoccupation majeure pour le Burkina Faso[12]face aux divers facteurs de risques mettant en péril la vie privée des citoyens. En effet, avec le développement des technologies de l'information et de la communication[13], un tel traitement a pris une nouvelle dimension en raison des ressources informatiques, non seulement la quantité des données traitées a accru, mais surtout le traitement

[11] [11]La protection de la vie privée est l'ensemble des mesures techniques visant à assurer le respect du droit à la vie privée.

[12] Il existait au Burkina Faso avant l'adoption de la LPDP n°010 du 20 avril 2004, des législations du droit commun qui régissaient la vie privée et des données personnelles des citoyens tels que le code civil, la responsabilité civile et le code du travail etc.…

[13]La Technologie de l'Information et de la Télécommunication sont diverses et échappent, de ce fait, à une définition précise. De manière approximative, elles s'étendent, conformément à l'article 1er de la Directive C/dir/1/08/11 du 19 Aout 2011 portant lutte contre la cybercriminalité dans l'espace CEDEAO comme « les technologies employées pour recueillir, stocker, utiliser et envoyer des informations incluant celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication »

de ces dernières est multiforme mettant en marge la protection effective de la vie privée des personnes concernées par le traitement[14] parce qu'il est devenu facile de modifier les données, de les effacer ou d'amputer une partie de celles-ci sans laisser des traces. Il est également aisé de stocker des grandes quantités de données dans de grosses bases de données et d'opérer des rapprochements entre, d'une part, des données de la même base, et d'autre part, des données de bases différentes.

Dans un tel contexte, la protection de la vie privée est menacée car l'utilisation des Technologies de l'Information et de la Communication (TIC) à des fins de traitement des données fait courir à l'individu le risque de perte de contrôle sur les informations relatives à sa personne[15].En effet, cette protection ne s'étend pas seulement du « droit d'être seul » ou du droit à l'intimité dans la vie, c'est-à-dire une vie cachée, tranquille, choisie ;elle implique également « la maitrise par l'individu de l'information qui circule à son propos, de la maitrise de son image informationnelle »[16] Pour cela, le Burkina Faso a adopté une loi n° 010 du 20 avril 2004 portant protection des données à caractère personnel pour la mise en œuvre de la protection des données d'utilisateurs à caractère personnel à l'image de la loi française de 1978 révisée par la loi de 2004 portant protection des données à caractère personnel(LPDP)[17]. Cependant, la protection effective des données à caractère personnel reste une lettre bois mort puisque les personnes concernées sont toujours victimes à cause de la multiplication accrue des programmes d'ordinateurs et des applications mobiles qui constituent des moyens de collecte des données d'utilisateurs à caractère personnel rendant difficile d'identifier l'auteur de la collecte des données ainsi que leur réutilisation éventuelle.

L'objectif assigné à la Commission de l'Informatique et des Libertés (CIL) créée par cette loi, est de protéger les droits des personnes concernées par le traitement afin d'éviter que leur intimité à la vie privée ne soit menacée[18]. En outre, elle doit exercer des contrôles auprès des entreprises d'internet ou de collecte de données à caractère personnel afin d'éviter toute exploitation abusive des données personnelles. En revanche, les personnes concernées sont confrontées toujours à des difficultés liées à la protection de leurs données à caractère personnel dont collectent les responsables de traitement. Ce qui justifie une violation persistante des droits des personnes concernées par le traitement sur les programmes d'ordinateurs au Burkina Faso.

[14]D.W. KABRE, Droit des technologies de l'information et de la communication, Burkina Faso, OFF PROD, 1ère éd. 1er janvier 2017, p.106.
[15] D. W. KABRE, Droit des technologies de l'information et de la communication, op.cit., p.106.
[16] M.H. BOULANGER et C. TERWANGNE, « internet et respect de la vie privée », in E. MONTERO (éd) internet face au droit, extrait des cahiers du CRID, n°12, p.192.
[17] La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés fut la pionnière française en matière de protection des données.
[18] Article 37 de la LPDP.

Il se pose par ailleurs le problème de réutilisation des données à caractère personnel des personnes concernées sur les logiciels au Burkina Faso sans leur consentement. Cette étude se veut être une contribution à la recherche des solutions à ces difficultés.

Pour ce faire, nous avons décidé d'étudier le cas spécifique de MTOPO[19] PAYEMENT SOLUTIONS BF et ses clients. Le choix de cette société se justifie par le fait que nous y avons effectué notre stage où nous avons constaté qu'elle dispose d'un serveur Microsoft qui collecte les données à caractère personnel des usagers des transporteurs terrestres de personnes dans ses rapports contractuels avec ses clients ,notamment les compagnies de Transport Sana Rasmané (TSR) et Transport RAHIMO où nous avons tenté d'accomplir des formalités préalables à la mise en œuvre des traitements auprès de la Commission de l'Informatique et des Libertés du Burkina Faso par la collaboration du Directeur général MTOPO PAYMENT SOLUTIONS BF. En fin, ce choix se justifie par le fait que l'entreprise dispose d'une technologie particulière en matière de traitement de données à caractère personnel au Burkina Faso.

MTOPO PAYEMENT SOLUTIONS BF a mis à la disposition de ces compagnies de transport terrestre de personne, notamment Transport Sana Rasmané (TSR) et RAHIMO TRANSPORT en vertu d'une licence d'exploitation d'un logiciel en mode SAS[20] (software as a service) permettant à ces dernières de gérer leurs activités telles que la vente des tickets, la réservation des tickets en ligne par les voyageurs, la gestion des bagues et des colis, la gestion des parkings ainsi que l'embarquement. Afin de profiter au mieux de l'environnement personnalisé, les voyageurs sont amenés à dévoiler énormément d'informations sur eux-mêmes, sans toujours mesurer le risque associé.

Pour l'exécution de ces activés, les compagnies de transport collectent les noms, prénoms, numéros de téléphone et les adresses e-mail des voyageurs qui constituent des données à caractère personnel. Les voyageurs sont obligés de transmettre ces informations personnelles potentiellement sensibles, y compris le compte mobile money[21].

Pour l'année 2018 TSR a enregistré environ 3 000 000 voyageurs soit 8334 voyageurs par jour dans la ville de Ouagadougou. RAHIMO TRANSPORT a enregistré dans la même année environ 1 080 000 voyageurs soit 300 voyageurs par jour dans la ville de Ouagadougou.

[19] MTOPO signifie en moré « trouver une solution à une situation donnée. »
[20] Le logiciel en tant que service désigne un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur.
[21] Ce que nous avons constaté lors de la vente des tickets aux voyageurs au TSR et RAHIMO TRANSPORT depuis mai 2018.

Courant mois de janvier -février 2019, TSR a enregistré 5 400 000 voyageurs soit 9000 voyageurs par jours dans la ville de Ouagadougou. RAHIMO a enregistré 24 000 voyageurs soit 400 voyageurs par jour dans la ville de Ouagadougou.

Toutes ces données personnelles sont hébergées dans le serveur de la société MTOPO PAYEMENT SOLUTIONS BF. Seules les compagnies de transport en tant qu'administrateurs doivent accéder aux données collectées. Cependant, MTOPO se borne à configurer les données hébergées sans avoir un droit d'accès de ces données si ce n'est qu'avec le consentement exprès des compagnies de transport qui en sont les propriétaires.

Vu le nombre de plus en plus élevé de traitements automatisés de données personnelles hébergées et l'hégémonie de MTOPO en matière d'hébergement des données d'utilisateurs au Burkina Faso, il faut se poser la question de savoir si les données à caractère personnel des personnes concernées sur le logiciel CONEKTO TRANSPORT ne sont pas détournées de leur finalité.

La problématique qui vient d'être posée nous oblige à justifier le choix de notre thématique.

2. La justification du choix du thème

Le choix de ce thème obéit à une exigence académique à savoir celle de produire un mémoire de fin de cycle de formation. C'est dans cette optique que nous avons opté de nous intéresser à la problématique de la protection des données à caractère personnel sur les programmes d'ordinateurs au Burkina Faso à travers le cas spécifique du logiciel CONEKTO TRANSPORT impliquant MTOPO PAYMENT SOLUTIONS BF, TSR et RAHIMO TRANSPORT. Les personnes concernées sont pour la plupart confrontées à des difficultés de protection de leurs données à caractère personnel. Nous pourrions résumer, pour ainsi dire, les raisons du choix du thème de la manière suivante :

D'abord, les voyageurs sont confrontés à des difficultés de protection de leurs droits et ils se retrouvent victime de la violation par les responsables de traitement des données à caractère personnel. Cette situation est en contradiction avec l'objet de la Loi portant Protection des Données à caractère Personnel (LPDP) et de la Commission de l'Informatique et des Libertés (CIL) qui est de veiller à la protection des données à caractère personnel à travers l'encadrement juridique et institutionnel de la mise en œuvre des traitements des données à caractère personnel. La présente étude entend contribuer modestement à la recherche des causes profondes de cette situation.

Ensuite, face aux difficultés de protection des données à caractère personnel des voyageurs, cette étude participera à réduire les violations de la vie privée des personnes concernées par la formulation de proposition tendant à l'amélioration de la protection de la vie privée des voyageurs des compagnies de transport TSR et RAHIMO et en même temps à la promotion de la législation en matière de protection des données à caractère personnel au Burkina Faso.

Après avoir posé la problématique et justifié le choix du thème, il convient à présent de se focaliser sur les objectifs et les questions de recherches.

B. Les objectifs et les questions de la recherche

Nous déclinerons dans cette rubrique les objectifs recherchés à travers l'étude (1) et les différentes questions que nous nous posons dans le cadre de la recherche (2).

1. Les objectifs de la recherche

Cette étude vise un objectif général (a) et plusieurs objectifs spécifiques (b).

a. L'objectif général de la recherche

Le principal objectif poursuivi à travers cette étude consiste à faire en sorte que les données à caractère personnel collectées des personnes concernées par le traitement sur le logiciel CONEKTO TRANSPORT ne soient pas utilisées à des finalités autres que celle pour lesquelles elles ont été collectées.

b. Les objectifs spécifiques

De façon spécifique, notre recherche consiste à :

- ✓ Appréhender le niveau de protection des données à caractère personnel des voyageurs sur le logiciel CONEKTO TRANSPORT par MTOPO PAYMENT SOLUTIONS BF et les compagnies de transport de personnes (RAHIMO et TSR) ;
- ✓ Apprécier les dispositifs mise en place par les compagnies de transports et MTOPO PAYEMENT SOLUTIONS BF en vue de la protection des données à caractère personnel des passagers sur le logiciel CONEKTO TRANSPORT ;

- ✓ Informer les voyageurs de leurs droits sur la protection de leurs données à caractère personnel sur le logiciel CONEKTO TRANSPORT.

Dans le souci d'atteindre les objectifs que nous nous sommes fixés, il est nécessaire de se poser un certain nombre de questions.

2. Les questions de recherche

Les objectifs que nous nous sommes fixés appellent une question principale et des questions secondaires. La question principale peut être formulée de la manière suivante : Les données à caractère personnel des personnes concernées sur le logiciel CONEKTO TRANSPORT ne sont-elles pas détournées de leur finalité ?

Cette question principale fait appel à d'autres questions secondaires. Celles-ci confirmeront ou infirmeront les différentes hypothèses qui sont formulées. Ces questions secondaires sont les suivantes :

- ✓ Les entreprises exploitant le logiciel CONEKTO TRANSPORT protègent-elles efficacement les données à caractère personnel des voyageurs ?
- ✓ Quelles sont les relations qui existent entre les différents acteurs dans le but d'assurer une meilleure protection des données collectées ?
- ✓ Quels sont les moyens mis à la disposition des personnes concernées par les responsables de traitement dans la protection de leurs données personnelles collectées ?

Pour apporter des réponses à ces différentes interrogations, il est indispensable pour nous de préciser l'intérêt de notre étude, de formuler les hypothèses de recherche et de définir les concepts clés.

Paragraphe II : L'intérêt, les hypothèses de recherche et le cadre conceptuel

A. L'intérêt et les hypothèses de recherche

L'intérêt (1) ainsi que les hypothèses de recherches (2) retiendront notre attention dans cette rubrique.

1. L'intérêt de la recherche

L'utilité de la recherche réside à plusieurs niveaux. D'abord, parce qu'il n'y a pas d'études sur la thématique au Burkina Faso. Bien que des rapports publics et séminaires menés par la CIL l'aient abordé. De même, plusieurs auteurs ont fait des recherches sur la protection des données à caractère personnel mais dans d'autres domaines. Aucune étude sur la protection des données à caractère personnel sur les logiciels n'a été effectué au Burkina Faso .Ensuite, notre recherche permettra une meilleure connaissance du niveau de protection des données à caractère personnel des voyageurs par MTOPO et les compagnies de transport terrestre (TSR et RAHIMO) .Enfin, l'étude pourrait permettre d'avoir une idée sur les difficultés auxquelles sont confrontés les voyageurs dans la protection de leurs données personnelles sur le logiciel CONEKTO TRANSPORT.

L'intérêt de la recherche qui vient d'être décliné, va s'appuyer sur des hypothèses qui seront confirmées ou infirmées dans le cadre de cette recherche.

2. Les hypothèses de recherche

Pour mieux appréhender si les données à caractère personnel des voyageurs, en général, et ceux de RAHIMO et TSR, en particulier, sont détournées de leur finalité initiale sans leur consentement, notre étude sera basée sur une hypothèse principale(a) et des hypothèses secondaires(b)

a. L'hypothèse principale

« La principale source de violation de la vie privée des voyageurs est le détournement de la finalité des traitements des données personnelles autres que celle pour laquelle elles ont été collectées par les compagnies de transport ».

A travers cette hypothèse principale, nous pouvons formuler des hypothèses secondaires.

b. Les hypothèses secondaires

- ✓ Les entreprises qui collectent les données à caractère personnel des voyageurs ne les protègent pas efficacement ;
- ✓ Il n'existe aucune relation entre les différents intervenant sur le logiciel CONEKTO TRANSPORT dans le but de la protection collective des données à caractère personnel des voyageurs ;
- ✓ Les voyageurs ne sont pas informés de leurs droits à la protection de leurs données personnelles collectées par les responsables des traitements.

C. Le cadre conceptuel

C'est le lieu pour nous de définir les concepts clés de notre thématique. Il s'agit entre autres des termes suivants :

Protection des données d'utilisateurs à caractère personnel : Dans sa thèse de doctorat intitulé « *protection des données personnelles coté utilisateurs dans le e-commerce », KEIRA Dari BEKARA définit la protection des données personnelles comme « l'ensemble des mesures techniques visant à assurer le respect du droit à la vie privée, limiter l'accès aux données de la sphère privée d'un utilisateur explicitement représenté sous forme numérique et mises en jeu dans le cadre d'une application informatique* »[22]. Il apparaît donc que les données personnelles ne sont qu'une partie de la sphère privée. La protection de ces données ne constitue qu'une partie de la protection du droit à la vie privée, même si restreinte au domaine numérique. En revanche, la protection de la vie privée, on l'a vu, n'intervient donc pas exclusivement dans le cadre d'applications informatiques. La notion de sphère privée apparaît dans toutes les activités humaines à partir du moment où elles ont une dimension sociale[23].

Donnée à caractère personnel : Suivant les textes relatifs à la protection des personnes à l'égard de l'utilisation des informations les concernant, il est généralement fait référence aux expressions « *données nominatives », « données personnelles », « données à caractère personnel »*[24].

[22] K. D. BEKARA, Protection des données personnelles coté utilisateurs dans le e-commerce, France, HAL, thèse, éd.2 juin 2014, p. 36.

[23] Idem p. 37.

[24] L'expression « donnée personnelle » est utilisée de façon elliptique pour désigner les « données à caractère personnel

En France, la loi pionnière du 06 janvier 1978[25] se referait, ainsi, initialement aux données nominatives[26].D'autres textes internationaux adoptaient, cependant, l'expression de donnée à caractère personnel. C'est le cas de la convention du Conseil de l'Europe pour la protection des personnes à l'égard des traitements automatisés des données à caractère personnel[27]. Si les deux expressions de « *donnée nominative* » et « donnée à caractère personnel » ont pu coexister dans la loi française, c'est lors de la modification en 2004, pour transposer une directive communautaire que l'expression donnée à caractère personnel sera généralisée. En effet la loi informatique et liberté modifiée se réfère désormais aux données à caractère personnel. L'ancien article 4 de la loi Informatique et libertés considérait comme « *nominatives... les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent* ».Le nouvel article 2 définit les données à caractère personnel comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres». L'objet de la protection visée par ces deux dispositions est donc bien l'information relative à des personnes physiques identifiables. Il n'y a pas de différence, au fond, quant au contenu de ces deux expressions qui désignent toutes, des informations permettant directement ou indirectement d'identifier les personnes physiques auxquelles elles se rapportent. Si l'expression « donnée nominative »* avait l'inconvénient de se focaliser sur le nom en réduisant par la même les moyens d'identification des personnes, l'expression « *données à caractère personnel* » est plus neutre et a l'avantage d'indiquer que sont concernées toutes les informations relatives à la personne physique et non exclusivement à celles comportant le nom[28].

Selon le Groupe de l'article 29[29] sur la protection des données personnelles, le concept de données à caractère personnel est fondé sur quatre éléments principaux à savoir : « *toute information », « concernant », « personne physique », « identifiée ou identifiable »*

La Loi portant Protection des Données à caractère Personnel(LPDP) et l'Acte additionnel A/SA.1/01 du 16 février 2010 relatif à la protection des données personnelles à

[25] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi est souvent appelée loi « Informatique et libertés ».
[26] Voir notamment l'ancien article 4 de la Loi Informatique et Libertés.
[27] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981. Cette Convention est souvent dite « Convention 108 ». Voir également, ONU (Organisation des nations unies), Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, 14 décembre 1990.
[28] L'intérêt de distinction entre donnée nominatives et données à caractère personnel.
[29] Groupe de protection des personnes à l'égard des traitements de données à caractère personnel ou « Groupe de l'article 29 ». Le « Groupe de l'article 29 » a été créé par la directive 95/46/CE du Conseil de l'Europe 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.

l'image de la loi française sur la loi informatique[30] définissent la donnée à caractère personnel comme toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques propres leur identité physique, psychologique, psychique économique, culturelle ou sociale.

Le nouveau règlement de l'Union Européenne en son article 4 alinéa 1 sur la protection des données personnelles, définit de manière précise les données à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable* »[31]. Il s'agit d'une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. La philosophie du règlement étant la protection des données personnelles des citoyens de l'Union Européenne, le règlement s'applique uniquement aux personnes physiques. Ainsi, sont exclues les données à caractère personnel relatives aux personnes morales[32] et, en particulier, aux entreprises dotées de la personnalité juridique et celles relatives aux personnes décédées[33].Il faut au préalable constater qu'il s'agit d'informations se rapportant à des personnes dont l'utilisation peut porter préjudice et nécessitent une protection à cet égard. Au sujet de la presse électronique, Mme Mallet-Poujol considère, ainsi, que « *c'est tant le contenu éditorial de la publication qui est susceptible de nuire à autrui que l'existence et la persistance de certaines données sur la toile. Il n'y a pas forcément de risque d'atteinte à la vie privée mais accumulation de données, pour certaines anodines, mais qui, rassemblées, peuvent être de nature à porter préjudice aux personnes concernées* ».

Programme d'ordinateurs : Le programme d'ordinateur, appelé également « *logiciel* » est « *l'ensemble d'instructions exprimées par des mots, des codes, des schémas ou par toute autre forme pouvant, une fois incorporée dans un support déchiffrable par une machine, faire accomplir ou faire obtenir une tache ou un résultat particulier par un ordinateur ou par un*

[30] Il s'agit respectivement de l'article 2, art. 2 et art.1 de la loi n°010 du 20 avril 2004 portant protection des données à caractère personnel, de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés et l'Acte additionnel A/SA.1/01 du 16 février 2010 relatif à la protection des données personnelles

[31] Article 4, al. 1er du Règlement 2016/679.

[32] En principe, les personnes concernées par la protection légale sont les personnes physiques. A contrario, les personnes morales se trouvent exclues du champ de cette protection. Toutefois, dans certaines situations, la loi trouvera à s'appliquer s'agissant par exemple des personnes physiques représentants légaux de personnes morales lorsque celles-ci sont nominativement désignées dans un fichier.

[33] Sur ce dernier point étonnant, notamment pour des données médicales qui pourraient concerner des apparentées vivantes, notons que le règlement permet aux Etats Membres de prendre les dispositions qu'ils estimeront utiles.

procédé électronique capable de faire de traitement de l'information »[34].Il résulte de cette définition que deux éléments caractérisent le programme d'ordinateur[35].Il s'agit d'une composante textuelle(code source) et un dispositif permettant l'accomplissement de certaines taches(codes objets).

Le logiciel, en tant que, programme d'ordinateur est protégé par le droit d'auteur[36]sous certaines conditions par le droit des brevets[37] .

Le logiciel CONEKTO TRANSPORT : selon le Directeur Général de MTOPO PAYEMENT SOLUTION BF dans le protocole de test CONEKTO TRANSPORT, le logiciel CONEKTO TRANSPORT est défini comme « *une plateforme de Gestion de compagnie de transport routier dénommée CONEKTO TRANSPORT permettant à tout client détenteur d'une licence d'utilisation d'avoir une solution de gestion de toute son activité* ». Il précise également que c'est un logiciel en mode SAS (Software As a Service), c'est-à-dire que le logiciel, en tant que service désigne un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent librement le service en ligne ou, plus généralement, payent un abonnement périodique. Ce logiciel permet aux compagnies de transport de gérer complètement leurs activités, d'imprimer des tickets de voyages, l'enregistrement des passagers, l'imprimer des étiquettes de colis et de bagages, l'embarquement des passagers et le traçage des colis et des bagages. Il permet aux voyageurs d'effectuer les réservations des tickets de voyage en ligne à travers une application mobile NTERI[38] qui est mise à leur disposition par MTOPO PAYEMENT SOLUTIONS BF.

La définition des concepts clés de notre thème nous conduit à faire un tour des différents écrits ayant trait à l'objet de notre étude.

[34] point 8) du lexique annexé à la loi n°032-99 /AN du 22 décembre 1999 portant protection de la propriété littéraire et artistique.

[35] D.W. KABRE, Droit de la technologie de l'information et de la communication, op.,cit., p.12.

[36]« Comme tout œuvre artistique et littéraire, le logiciel n'est digne de protection que s'il présente une certaine originalité permettant d'individualiser son auteur », D. W. KABRE, Droit de la Technologie de l'Informatique et de la télécommunication, op.,cit., p.11 et un arrêt de la cour de cassation française du 17 octobre 2012.

[37] Le logiciel en tant que tel ne peut accéder à la protection par le droit de brevet puisqu'il n'implique aucune invention, toutefois lorsqu'il est incorporé en un procédé industriel, il peut être breveté.

[38] Cette application a été détournée par le chef de projet informatique de MTOPO en Aout 2018.Des procédures judiciaires sont déclenchées à l'encontre du délinquant.

Section II : Cadre méthodologique de l'étude

Le cadre méthodologique de la recherche sera présenté au moyen de deux paragraphes. Le premier paragraphe présente le champ de l'étude, à savoir MTOPO PAYMENT SOLUTIONS BF, la CIL, la société TSR, RAHIMO TRANSPORT, le public cible et l'échantillonnage. Le deuxième paragraphe sera axé sur la méthodologie de collecte, de traitement et d'analyse des données.

Paragraphe I : Le champ de l'étude, le public cible et l'échantillonnage

Dans ce paragraphe, il sera question de décrire le champ de notre étude (A) et d'identifier le public cible et l'échantillon choisi pour la vérification de nos hypothèses (B).

A. Le champ de l'étude

Nous procèderons, d'abord, par un bref aperçu de MTOPO PAYEMENT SOLUTIONS BF, de la CIL (1), puis par une présentation des compagnies de transport terrestre de personnes à savoir TSR (2)

1. Bref aperçu de MTOPO PAYEMENT SOLUTION BF et la CIL

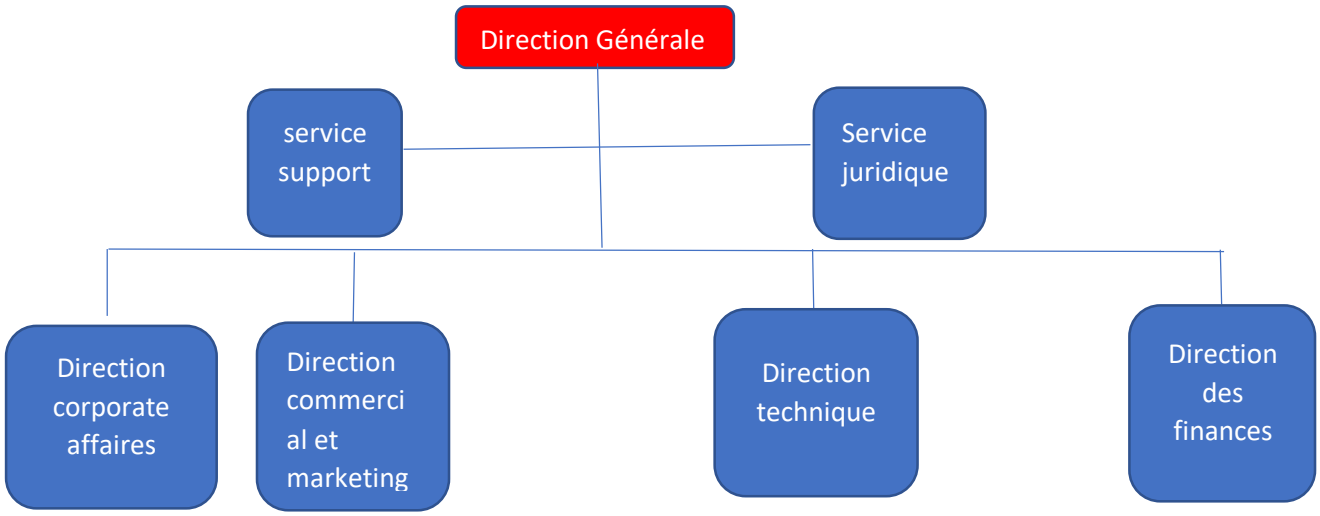
a. Bref aperçu de MTOPO PAYEMENT SOLUTION BF

MTOPO PAYEMENT SOLUTIONS BF est un établissement de technologie. Elle est créée au Burkina Faso en 2017 et s'est constitué en une Société à Responsabilité Limitée (SARL), avec un capital social de 10 000 000 FCFA. Son siège social est situé à OUAGA 2000, 11 BP 606 Ouagadougou, et elle est immatriculée au Registre du Commerce et du Crédit Mobilier sous le numéro BFOUA 2017 B2711. Elle est une société unipersonnelle, c'est-à-dire, constituée d'un seul associé. Elle a son siège à Ouaga 2000 sur l'avenue PASCAL ZABRE. Son Directeur Général actuel est Monsieur Seny GANEMTORE, l'associé unique.

Missions : MTOPO PAYMENT SOLUTIONS a pour mission de mettre en œuvre le système de Massachusetts Institute Technology (MIT) en Afrique en général et au Burkina Faso en particulier « *en Connectant les entreprises à leur environnement* » en vue de débloquer leur potentiel de croissance. Et ceci :

- ✓ en permettant aux petites et moyennes entreprises africaines de combler leur retard et d'être compétitives face à leur environnement en évolution rapide ;
- ✓ en équipant des commerçants avec des outils de gestion et des outils d'analyse de classe mondiale, et en les insérant dans un écosystème de paiement sans numéraire ; via une plate-forme de traitement des paiements sécurisés ;
- ✓ en assurant des paiements sans numéraire et transparents partout à travers une passerelle unique ;
- ✓ en créant des partenariats et des synergies avec tous les acteurs : Opérateurs mobiles money, banques, commerçants et utilisateurs.
- ✓

Organigramme de septembre 2018 :



b. Bref aperçu de la Commission Informatique et Libertés

La Commission de l'Informatique et des Libertés (CIL) est une Autorité administrative indépendante, créée par la Loi N°010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel. Elle est située à Ouaga 2000 sur Boulevard Mouammar Kadhafi, 01BP 1606 Ouagadougou. Elle est présidée par Marguerite OUEDRAOGO/BONANE.
Elle est fonctionnelle depuis décembre 2007.

La commission compte neuf (09) membres, nommés en conseil des ministres pour un mandat de cinq ans renouvelables une fois. Elle se compose ainsi qu'il suit :

- Deux (02) magistrats représentant le pouvoir judiciaire ;
- Deux (02) députés représentant l'Assemblée Nationale ;
- Deux (02) personnalités issues des associations nationales œuvrant dans le domaine des droits humains ;

- Deux (02) personnalités issues des associations nationales de professionnels de l'informatique ;
- Une (01) personnalité représentant l'exécutif désignée par le Président du Faso.

La CIL est dirigée par un président nommé par le Chef de l'Etat parmi les membres. Le président est secondé par un Vice-président élu par ses pairs.

Ses principales missions sont :

- Informer les personnes de leurs droits et obligations en matière de traitement des données à caractère personnel ;
- Réguler en veillant au respect des formalités préalables à tout traitement de données à caractère personnel ;
- Contrôler la conformité des traitements aux dispositions de la loi N° 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel quel qu'en soit le responsable ;
- Protéger les droits des personnes ;
- Anticiper en proposant au Gouvernement toutes mesures législatives ou réglementaires de nature à adapter la protection des libertés à l'évolution des TIC.

Pour réussir sa mission, la CIL dispose d'un pouvoir de contrôle des organismes publics et privés, et un pouvoir de sanction et de dénonciation au parquet des contrevenants à la loi portant protection des données à caractère personnel.

La Commission, pour son fonctionnement, s'appuie sur les services administratifs suivants :

- Le Secrétariat général (SG) ;
- La Direction de l'Expertise Technique et du Contrôle (DETC) ;
- La Direction des Affaires Juridiques et du Contentieux (DAJC) ;
- La Direction des Affaires Administratives et Financières (DAAF) ;
- La Direction de la Communication et des Relations Publiques (DCRP).

2. Une présentation du TSR

La société Transport Sana Rasmané en abrégé TSR[39], est née en 1998 sous forme d'une entreprise individuelle. A partir de 2002, elle prendra la forme d'une Société à Responsabilité Limitée (SARL) avec une flotte de plus d'une centaine de Bus ainsi qu'une ouverture désormais tournée vers l'International.

[39] Voir « http://www.groupe-tsr.com/spip.php?rubrique4 « consulté le(22/02/2019 à 12h 20).

Quinze années après sa création, elle a multiplié sa flotte de Bus, élargie sa cartographie nationale en déployant ses gares et ses agences dans toutes les régions du Burkina Faso. Sa forme sociale ainsi que son capital social ont également évolué. Société à Responsabilité Limité avec un capital de 5 000 000 de Francs CFA, TSR est devenue en 2013 une Société Anonyme avec une augmentation notable de son capital qui a atteint 200 000 000 FCFA. La société TSR emploie plus de quatre cents (400) employés contractuels et prestataires confondus. La Société TSR est coiffée par un Directeur Général qui est secondé par un Directeur Général Adjoint ; le service financier de TSR est représenté par un Chef Comptable et un Contrôleur Interne. Les agences ou les gares sont administrées par un Chef d'Agence ou de Gare, un comptable, un ou plusieurs guichetiers. TSR dispose en outre d'un service de Ressources Humaines et Juridique. L'ensemble de son administration fonctionne suivant un manuel de procédure établi pour sa bonne marche.

Aujourd'hui, plus qu'hier encore, le Burkina Faso compte énormément sur les services rendus par la société TSR pour contribuer au désenclavement des populations et au développement de son commerce. La société TSR se place parmi les plus compétitives dans le secteur du Transport au Burkina Faso ; aussi est- elle devenue le leader national dans le domaine du transport avec un trafic routier très intense : à chaque heure, un Départ et une Arrivée !

Le Siège principal de TSR se trouve dans la capitale du Burkina Faso. Il est situé dans le Quartier commercial de Ouagadougou appelé « Gounghin ».

Monsieur SANA Rasmané est le fondateur de TSR. Il est coactionnaire avec Monsieur SANA Idrissa.

B. Le public cible et l'échantillonnage

Cette rubrique a pour objet de déterminer le public cible de notre étude (1) et de préciser l'échantillon qui sera choisi pour mener l'enquête (2).

1. Le public cible

Notre travail est axé sur quatre (04) groupes de personnes notamment les responsables des compagnies de transport (TSR et RAHIMO TRANSPORT), les usagers des compagnies de transport terrestre de personnes, les responsables de la CIL et les responsables de MTOPO PAYEMENT SOLUTIONS BF. Le choix porté sur ces personnes se justifie par le fait qu'elles sont au cœur de la problématique que soulève notre thème.

Par exemple les usagers des compagnies de transports peuvent nous renseigner sur les difficultés rencontrées dans le cadre de la protection de leurs droits sur le logiciel CONEKTO TRANSPORT et leur ignorance quant à l'existence de la loi sur la protection des données personnelles. Les responsables de MTOPO PAYMENT SOLUTIONS BF et les compagnies de transport pourront nous renseigner sur les mesures organisationnelles et techniques mises en place dans le cadre de la protection des données personnelles et les différents traitements effectués sans le consentement des voyageurs contrevenant le principe de respect de la finalité des traitements mettant en jeu la vie privée des voyageurs.

Le public cible étant détecté, il faut préciser notre échantillon ou encore l'ensemble des individus qui seront concernés par l'enquête.

2) L'échantillon de la recherche

Parmi ces personnes ciblées, nos outils de collecte des données seront adressés à un échantillon de 1010 personnes réparties comme suit :

- ✓ 01 responsable de la société MTOPO PAYEMENT SOLUTIONS BF
- ✓ 03 responsables de la CIL
- ✓ 03 responsables du TSR
- ✓ 03 responsables de RAHIMO TRANSPORT
- ✓ 200 voyageurs de RAHIMO TRANSPORT
- ✓ 800 voyageurs de TSR.

Nous avons opté pour un échantillon aléatoire en ce que nous estimons que les réponses qui seront données reflètent la réalité sur le terrain. Le public cible et l'échantillonnage étant précisés, il convient maintenant de dérouler la méthodologie de collecte des données ainsi que les difficultés et les limites de la recherche.

Paragraphe 2 : La méthode, les instruments de collecte des données et les difficultés, limites de la recherche.

Nous aborderons d'une part la méthode et les instruments de collecte des données (A) et d'autre part les difficultés et limites de la recherche(B).

A. La méthode et les instruments de collecte des données

Dans tout travail de recherche les informations sont recueillies par l'utilisation d'une méthode (1) précise et aux moyens d'instruments de collecte de données (2).

1. La méthode de collecte des données

En ce qui concerne la collecte des données, nous avons opté pour la méthode quantitative avec pour objectif de recueillir des informations sur les différents aspects de notre thème. Il s'agit entre autres :

- ✓ Les difficultés rencontrées par les voyageurs dans le processus de protection de leur droit ;
- ✓ Les mesures techniques et organisationnelles mises en place par les responsables de traitement dans la protection des droits des personnes concernées afin d'apprécier le niveau de protection des données personnelles ;
- ✓ La réutilisation des données personnelles à d'autre fin autre que celle prévue dans le contrat ;
- ✓ La non information des voyageurs de leurs droits sur la protection des données à caractère personnel ;
- ✓ Le niveau de coopération entre l'entreprise de technologie et ses clients dans le processus de protection des données d'utilisateurs à caractère personnel.

2. Les instruments de collecte des données

Plusieurs instruments sont utilisés dans le cadre de la recherche appliquée. Nous en avons choisi deux (2). Il s'agit des questionnaires et des guides d'entretien semi-dirigé.

Les questionnaires ont été conçus à l'adresse des voyageurs et quelques employés du TSR et RAHIMO TRANSPORT. L'utilisation de cet outil se justifie par le fait qu'il permet d'atteindre plusieurs individus en même temps. Son inconvénient est qu'il est susceptible de fournir des informations erronées. Par ailleurs, les questionnaires sont des outils qui facilitent la collecte de données quantitatives.

Pour ce qui est des informations recueillies auprès du Directeur Général de MTOPO PAYMENT SOLUTIONS BF et des compagnies de transport, des responsables des structures administratives et des personnes ressources, des guides d'entretien ont été élaborés à cet effet. Les guides d'entretien permettent de recueillir des données qualitatives.

Ils ont l'avantage de créer une certaine interaction entre l'enquêteur et la personne soumise à l'entretien. Cet outil permet une libre expression de l'enquêté qui peut revenir sur ses propos à tout moment. Mais l'entretien semi-dirigé exige la présence effective de l'enquêteur qui doit être attentif pour ne pas perdre le fil des échanges. Pour mener à bien un entretien semi-dirigé, il faut à l'avance soumettre aux intéressés un guide d'entretien afin que ceux-ci se préparent. Les données collectées subiront un traitement statistique à l'aide du logiciel Excel. Ces données feront l'objet d'une analyse qualitative et quantitative.

Dans le cadre de cette recherche, nous avons été confrontés à certaines difficultés.

B. Les difficultés et les limites de la recherche

Nous évoquerons d'abord les difficultés (1) puis les limites de cette recherche (2) dans cette rubrique.

1. Les difficultés de la recherche

Nous avons été confrontés à des difficultés tout au long de cette recherche. Il s'agit d'abord de l'indisponibilité des documents qui traitent de la problématique abordée dans cette œuvre. Plusieurs bibliothèques de la place ont été visitées sans succès, en raison du fait que, jusqu'à présent au Burkina Faso aucun écrit n'a abordé cette thématique ce qui nous a obligé à nous inspirer des mémoires et thèses onlines et à des supports numériques d'origine étrangère. Leur disponibilité aurait dû contribuer à l'amélioration de la qualité scientifique de notre document.

Par ailleurs, nous avons été confrontés à d'autres obstacles pendant la phase d'enquête sur le terrain. Certains acteurs clés de notre étude ne respectaient pas les rendez-vous qui nous ont été fixés. Ce qui ne nous a pas permis de disposer de certaines données afin de mener des analyses approfondies. Par exemple, les chefs de la société TSR et RAHIMO TRANSPORT n'ont pas voulu, au début, un entretien sur la protection des données personnelles. Ils arguent de ce que TSR et RAHIMO TRANSPORT ne sont pas les seules sociétés au Burkina Faso utilisant des données personnelles pour être la cible de nos recherches. C'est suite à nos négociations pendant plusieurs jours qu'ils nous ont reçus dans leur société. Malgré l'autorisation d'enquête et d'entretien, certains chefs d'entreprises, en raison de leur négligence ou d'indisponibilité n'ont pas pu nous recevoir pour des entretiens que nous avons sollicités.

Aussi, les questionnaires conçus afin de recueillir des données à même de nous aider à la vérification de nos hypothèses, ne nous ont pas été retournés en intégralité.

De même, les interrogatoires ont été faits à l'oral. Certains voyageurs approchés n'ont pas pu donner une réponse en raison de leur ignorance et de leur timidité.

La dernière difficulté à laquelle nous avons été confrontées est l'insuffisance des ressources financières. En effet, la reproduction des questionnaires, des guides d'entretien ainsi que l'impression du document finalisé n'ont pas été facile. Malgré ces difficultés, nous avons tenu à produire cette œuvre afin de contribuer à notre façon au développement du capital humain dans notre pays. Après ce bref rappel sur les difficultés de la recherche, nous allons à présent évoquer les limites de la présente étude.

2. Les limites de l'étude

Nous entendons, à travers cette étude, apporter notre part contributive à la résolution du problème de réutilisation des données personnelles à d'autres finalités autres que celle pour laquelle elles ont été collectées sans le consentement des personnes concernées.

De ce point de vue, nous sommes conscients que notre étude peut ne pas appréhender tous les aspects liés à cette problématique. Donc, nous ne prétendons pas à l'exhaustivité dans le cadre de nos différentes analyses.

En outre, la question de la protection des données personnelles nécessite un champ d'étude plus vaste. Mais compte tenu du temps et des ressources dont nous disposons, la recherche a été exclusivement consacrée au cas de MTOPO PAYMENT SOLUTIONS BF et les compagnies de transport. Par conséquent, il se posera sans doute un problème de généralisation des conclusions auxquelles nous sommes parvenues.

Le cadre théorique et méthodologique ayant été bouclé, nous passerons maintenant à l'étude de la notion de protection des données à caractère personnel au Burkina Faso.

CHAPITRE II- PROTECTION DES DONNEES A CARACTERE PERSONNEL EN DROIT BURKINABE.

Il est évident que le point de départ de tout travail juridique est constitué de sources formelles de droit. Nul ne peut, en effet, prétendre faire œuvre juridique en ignorant le postulat essentiel suggéré par le professeur Vittorio Villa pour qui, tout opérateur juridique doit, avant tout, connaître les paradigmes du droit positif. Pour ce faire, dans ce chapitre nous allons étudier, dans un premier temps, le cadre juridique de la protection des données personnelles (section I) et dans un second temps, les conditions d'utilisations des données à caractère personnel en droit burkinabé (section II).

Section I : Cadre juridique de la protection des données à caractère personnel.

Dans cette section, nous étudierons, d'une part, le cadre juridique international (paragraphe I), et d'autre part, le cadre juridique national (paragraphe II).

Paragraphe I : Le cadre juridique international

Il faut entendre par législation internationale toute règle de droit qui s'applique à deux (02) ou plusieurs États ou à plusieurs sujets du droit international. Notre étude est circonscrite à l'analyse de la législation burkinabè en matière de protection des données personnelles. Cependant, l'évocation des législations internationales nous permettra de faire une étude comparée de ces législations par rapport à la législation burkinabé.

Dans ce paragraphe, il sera question d'aborder la législation européenne (A) et la législation onusienne et africaine (B)

A. La législation Européenne

La législation européenne en matière de protection des données personnelles est consacrée par le Conseil de l'Europe (1) et par l'Union Européenne (2)

1. **Conseil de l'Europe**

En Europe, la consécration du droit au respect de la vie privée en tant que concept juridique intervient seulement à la suite de la seconde guerre mondiale et du développement conséquent des droits de l'Homme[40].Le droit au respect de la vie privée est inscrit comme un droit fondamental à l'article 8 de la Convention Européenne des Droits de l'Homme[41] (ci-après, « CEDH ») s'est indéniablement inspirée de l'article 12 de la Déclaration Universelle des Droits de l'Homme des Nations Unies[42] de 1948.Ce droit au respect de la vie privée comporte une double dimension: d'une part, le droit à l'intimité, c'est-à-dire le droit de ne pas laisser exposer publiquement des informations personnelles, et, d'autre part, un droit à l'autonomie personnelle selon lequel chacun peut mener sa vie comme il l'entend[43].Ainsi, la protection des données personnelles est consacrée par l'article 8 de la CEDH. L'article 8 paragraphe 2 de la CEDH admet des ingérences lorsqu'elles sont nécessaires à la sécurité nationale ou à la défense de l'ordre et à la prévention des infractions pénales dans une société démocratique[44].

La jurisprudence de la Cour européenne des droits de l'Homme accorde une attention particulière à l'égard de la confidentialité des données médicales et au rôle que joue le consentement du patient dans la divulgation de ses données. En effet, ces données constituent par leur nature des informations profondément intimes à propos de la vie privée du patient. En conséquence, il n'est permis de déroger au secret médical et à l'exigence du consentement du patient que dans des cas exceptionnels et après pondération des intérêts en présence[45]

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (connue sous le nom de Convention108), adoptée en 1981 par le Conseil de l'Europe est, jusqu'ici, la seule convention à vocation internationale[46]

---

[40] L. Marie, Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique, mémoire, LIEGE université, France, éd.2018, p.10.

[41] Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH) signée le 4 novembre 1950 à Rome par les Etats membres du Conseil de l'Europe et entrée en vigueur le 3 septembre 1953.

[42] Déclaration universelle des droits de l'homme adoptée le 10 décembre 1948 à Paris par l'Assemblée générale des Nations Unies. Cette déclaration n'a pas de portée juridique en tant que telle, elle n'a qu'une valeur de proclamation de droit.

[43] L.Marie, Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique, op., cit. p.10.

[44] L'article 8 de la Convention européenne des droits de l'Homme

[45] L'auteur poursuit avec une illustration de l'arrêt Z. c. Finlande, où la Cour a jugé que la révélation par des médecins d'un état de séropositivité d'une personne sans son consentement, alors que cette personne est contrainte par la justice à témoigner, ne peut se justifier que dans l'intérêt des poursuites pour homicide volontaire dirigées contre son mari suspecté de l'avoir contaminée. Cour eur.D.H. Z c. Finlande, 25 février 1997, req. n°22009/93.

[46] Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée le 28 janvier 1981 à Strasbourg par le Conseil de l'Europe. La convention compte actuellement 51 États Parties, à savoir les 47 États membres du Conseil de l'Europe et l'Uruguay, l'île Maurice, le Sénégal et la Tunisie. L'Argentine, le Burkina Faso, le Cap Vert et le Maroc ont également été invités à y adhérer et le Mexique vient d'en faire la demande.

Malgré une interprétation évolutive et dynamique de l'article 8 de la CEDH, le droit a besoin de s'adapter à la mutation sociétale et aux développements technologiques, pour faire en sorte de protéger de manière appropriée les individus[47]. Par conséquent, le Conseil de l'Europe adopte le 28 janvier 1981, une législation particulière à la protection des données personnelles, la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[48].En 1999, elle est modifiée afin de pouvoir permettre à l'Union Européenne d'y adhérer.

La Convention n°108 est le premier, et reste à ce jour, le seul instrument international contraignant ayant pour objet la protection des personnes contre l'usage abusif du traitement automatisé des données à caractère personnel. De par sa vocation universelle, elle dispose de la faculté de remédier à l'absence d'une convention mondiale dans ce domaine.

La Convention énonce les droits dont dispose l'individu sur ses données personnelles tels que le droit à l'information[49], le droit d'accès aux données[50], le droit à l'effacement[51] ainsi que les principes directeurs que les acteurs, tant privés que publics, doivent respecter lors du traitement des données, comme par exemple le principe de minimisation[52], de loyauté ou encore de proportionnalité[53]. Une partie est également consacrée au transfert des données hors Europe et aux données sensibles qui requièrent une protection particulière.

Après avoir évoqué la législation en matière de protection des données personnelles consacrées par le CE, nous étudierons celle de l'UE.

2. Union Européenne

L'UE a consacré des directives(a) et un nouveau règlement sur la protection des données à caractère personnel(b)

[47]J. RIDEAU, Les droits fondamentaux dans l'Union européenne, Bruxelles, Bruylant, 2009, p. 61.
[48] Convention n°108 précitée.
[49] Le droit à l'information signifie que la personne concernée a droit à être informé par le responsable des traitements des données le destinataire des traitements, la durée de la conservation des données ainsi que l'éventuelle utilisation des données non compatible avec la finalité initiale.
[50] Le droit d'accès aux données signifie que la personne concernée a le droit d'accéder à ses données personnelles auprès des responsables des données pour vérifier la conformité de traitement de ses données à la loi.
[51] Droit à l'effacement signifie que toute personne physique, dispose du droit de se faire communiquer toutes les informations le concernant dans un fichier et de faire rectifier ou supprimer les informations erronées.
[52] Le principe de minimisation signifie que la personne concernée a le droit d'obtenir du responsable du traitement pour la limitation du traitement.
[53] Principes de licéité à respecter lors du traitement sont des principes directeurs de traitement des données personnels tels que le consentement, respect de la finalité des traitements, délai de conservation des données….

a. Les directives relatives à la protection des données à caractère personnel

Directive 95/46/CE

Le 24 octobre 1995, la Commission adopte la directive 95/46/CE relative à la protection des données[54], avec un double objectif : assurer la libre circulation des données entre Etats membres tout en garantissant un niveau équivalent de protection des données dans toute l'Union. La directive énonce les différents principes de licéité à respecter lors du traitement de données personnelles.

Directive 2002/58/CE

La Commission européenne constate que la directive de 1995 est déjà dépassée et qu'elle ne peut plus faire face aux nouveaux défis posés par les nouvelles technologies qui permettent une collecte et un stockage toujours plus important des données personnelles .Au vu de l'essor des données qui transitent par voie électronique, la Commission européenne a adopté,, en 2002 la directive 2002/58/CE relative au secteur des communications électroniques afin d'émettre des règles plus détaillées et particulières à ce domaine[55]. La directive de 2002 règle notamment les questions relatives aux cookies[56]et au spamming[57]. Ainsi, la directive affecte directement sur les techniques de marketing des entreprises qui basent essentiellement leur politique commerciale sur une philosophie de personnalisation du client[58].Une fois les directive évoqués nous analyserons le RGPD.

b. Le nouveau règlement européen sur la protection des données à caractère personnel

C'est le règlement n°2016/679 dit Règlement général sur la protection des données (RGPD ou encore GnDPR en anglais, General Data Protection Régulation)[59].

---

[54] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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.

[55] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Notons que cette directive sera ensuite modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques.

[56] Les cookies informatiques ou « traceurs de connexion » sont « des fichiers textes stockés sur un terminal (ordinateur, smartphone) par exemple lors de la consultation d'un site internet, de la lecture d'un mail.

[57] Le spamming correspond à l'envoi massif de courriers électroniques non sollicités, le plus souvent à des fins publicitaires.

[58] L. Marie, Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique, op. ,cit., p.8.
14.

[59] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces

Ce texte de l'Union Européenne constitue aujourd'hui la référence en matière de protection des données à caractère personnel en raison du fait qu'elle renforce et unifie la protection des données des personnes concernées[60]. Dans la perspective de modernisation de la directive 95/46/CE, le nouveau règlement poursuit, comme objectif, le renforcement du contrôle de l'individu sur l'utilisation qui est faite de ses données, notamment en accentuant le rôle du consentement et le droit à l'information[61] .L'article 3 du RGPD précise que le Règlement s'applique aux traitements des données effectués dans le cadre des activités d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union ,que le traitement ait lieu ou non dans l'Union[62] .

Le règlement général sur la protection des données a été adopté le 27 avril 2016. Il est entré en vigueur le 25 mai 2018 et les dispositions sont directement applicables dans l'ensemble des Etats membres le 25 mai 2018. Il tend également à responsabiliser les autorités, les entreprises, et toutes autres entités traitant de données personnelles[63]. Dans cette optique, le règlement établit pour la première fois, en matière de protection des données, un arsenal de sanctions en cas d'entorse allant jusqu'à des amendes pouvant atteindre les 20 millions d'euros ou 2 à 4% du chiffre d'affaires[64]. Un vent de panique souffle sur les entreprises inquiètes de ne pas être en conformité avec le nouveau règlement[65]. On peut raisonnablement penser que ce nouvel élément va imposer le respect de la nouvelle législation.

Deux constats majeurs ont été à l'origine du RGPD[66] :

- ✓ L'inefficacité révélée, en 2012, des lois nationales et communautaires à protéger les données personnelles des citoyens européens ;
- ✓ L'affaire SNOWDEN : relative à une surveillance de masse des citoyens européens par les États-Unis.

données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) adopté le 27 avril 2016 et rentra en vigueur le 25 mai 2018.

[60] M. OUEDRAOGO / BONANE, présidente CIL Burkina Faso, aperçu Règlement général sur la protection des données personnelles et ses implications dans les pays hors union européenne, documentation burkinabé, 2018, p .11.

[61] COMMISSION EUROPEENNE, Communiqué de presse du 4 novembre 2010 : « Une approche globale de la protection des données à caractère personnel dans l'Union européenne ».

[62]Article 3 du nouveau RGPD.

[64] Cf. aperçu de M. OUEDRAOGO/BONANE sur les implications du Règlement général sur la protection des données personnelles, p.13.

[65] L.Marie, Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique, op.,cit. p.14.

[66]Cf. M. OUEDRAOGO/BONANE, sur les implications du Règlement général sur la protection des données personnelles, op.,cit. ,p. 11.

Le RGPD concerne tous les acteurs économiques et sociaux proposant des biens et services sur le marché européen, dès lors que leurs activités traitent des données personnelles des résidents de l'Union Européenne[67]. Seront donc concernés :

- les entreprises ;
- les associations ;
- les organismes publics, mais aussi-les entreprises dont le siège est hors de l'Union Européenne, mais qui opèrent au sein de l'Union européenne et sur les données des citoyens de l'Union Européenne ;
- enfin, les sous-traitants dont les activités entrent dans ce cadre.

L'objectif primordial du RGPD est de donner aux citoyens européens des avantages de contrôle et de visibilité sur leurs données privées, notamment pour savoir quelles sont les données personnelles collectées, où sont-elles stockées, à quelles fins, à qui sont-elles transférées et jusqu'à quand ? En un mot, elle vise à garantir la protection des données personnelles et de la vie privée des citoyens européens par tout responsable de traitement, quel que soit le pays d'origine[68].

Le principal enjeu pour les entreprises est de savoir, en un instant donné, où sont les données et comment pouvoir, sur simple demande, les collecter et les transmettre à la personne concernée[69]. Cela suppose que l'entreprise doit connaitre, à tout moment, les données dont elle dispose, leur localisation, l'objectif de leur collecte, leur mode de gestion, de stockage, de transfert et d'effacement.

Les principes directeurs du RGPD sont prévus aux articles 30 à 37 du RGPD. Les principes directeurs du RGPD sont prévus aux articles 30 à 37 du RGPD.Il s'agit du principe

[67] Article 3-1et 2 du RGPD.
[68] Idem
[69] Dans le même sens, article 12 -1 du RGPD.

de Accountabililty[70], du principe de Privance by design[71], du principe de Security by default[72] ,du principe de Data Protection Officers[73] (DPO)et le principe d'étude d'impact[74].

Il convient de relever que le RGPD vient engager davantage la responsabilité des responsables de traitement et celle des sous-traitants, renforcer les droits des personnes concernées, renforcer les sanctions pour la non-conformité. Il est une législation de référence mondiale puisqu'il protège sans failles théoriquement les personnes concernées. Enfin, l'une de ses particularités fondamentales est son applicabilité extraterritoriale[75]. En effet, il s'adresse à tous les pays du monde et vise à contraindre les géants du Net que sont les GAFAM[76] au respect des données personnelles des internautes. Après avoir évoqué le cadre juridique de l'Union Européenne, il nous a fallu souligner la législation onusienne et africaine.

B. Législation onusienne et africaine

Nous exposerons, dans un premier temps, la législation adoptée par les Nations Unies (1) et, dans un second temps, celle adoptée par l'Afrique (2).

1. La législation onusienne en matière de protection des données personnelles.

Des travaux importants ont été entrepris au sein des Nations Unies pour élaborer des principes directeurs en matière de protection des données grâce à l'impulsion de Louis Jointe rapporteur spécial en 1980 par la Sous-Commission des droits de l'homme (résolution 12 XXXIII). Ils ont abouti à des « *principes directeurs pour la réglementation des fichiers informatisés concernant des données à caractère personnel* » entérinés par la Sous-Commission des droits de l'homme dès 1983, puis adoptés par l'Assemblée Générale des

[70] L'Accountabililty qui introduit une logique de responsabilisation selon lequel, il revient à l'entreprise de prendre toutes les dispositions pour garantir sa conformité au RGPD et démontrer à l'Autorité de contrôle dont elle relève qu'elle a rempli ses obligations.

[71] Privacy by design signifie que la protection des données personnelles est prise en compte dès la conception du produit ou du service, notamment dans le système d'informations de l'entreprise, au sein d'une base de données, ou lors de la conception d'une application.

[72] Le principe de Security by default ou la sécurité par défaut consiste à renforcer le rôle de la sécurité dans le système d'information. En effet, le système d'information de l'entreprise doit être sécurisé à tous les niveaux, du physique au logique, avec par exemple, des contrôles d'accès ou des systèmes de prévention contre les failles éventuelles de sécurité ; l'entreprise doit être à mesure de déceler si son système d'information a été compromis et pouvoir y remédier en un temps record. Pour cela, elle doit limiter l'accès aux données personnelles, éviter les copies multiples et minimiser les données stockées.

[73] La désignation d'un Data Protection Officiers (DPO) ou délégué à la protection des données personnelles. Le DPO doit être associé aux différentes questions et problématiques de protection des données à caractère personnel de l'entreprise ; son rôle est de veiller à la conformité au RGPD des traitements effectués et d'être le point de contact avec les autorités de contrôle.

[74] La réalisation d'une étude d'impact : le RGPD recommande aux entreprises de réaliser une étude d'impact avant la mise en œuvre de nouveaux traitements de données personnelles, qui pourraient potentiellement présenter des risques d'atteinte aux droits et aux libertés individuelles.

[75] Le RGPD s'applique hors de l'Union Européenne.

[76] GAFAM signifie Google, Apple, Facebook, Amazon et Microsoft.

Nations Unies dans sa résolution 45/95 du 14 décembre 1990[77]. On retrouve une série de « principes concernant les garanties minimales qui devraient être prévues dans les législations nationales », notamment le principe de licéité et de loyauté, le principe d'exactitude, le principe de finalité, le principe d'accès par les personnes concernées, le principe de non-discrimination, le principe de sécurité, assortis de mécanismes de contrôle et de sanctions. Ainsi « *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* » (principe 8). Par ailleurs, la résolution vise l'application de ces principes directeurs aux fichiers détenus par les organisations internationales, la question, déjà sensible dans le cas d'Interpol, l'est plus encore aujourd'hui s'agissant des listes établies par le comité contre le terrorisme du Conseil de sécurité. Se fondant, lui aussi, très largement sur l'étude menée à bien par Louis Jointe dans le cadre de la Sous-Commission, le Comité des droits de l'homme, dans son observation générale n°16 de 1988, souligne que « *le rassemblement et la conservation, par des autorités publiques, des particuliers ou des organismes privés, de renseignements concernant la vie privée d'individus sur des ordinateurs, dans des banques de données et selon d'autres procédés, doivent être réglementés par la loi. L'État doit prendre des mesures efficaces afin d'assurer que ces renseignements ne tombent pas entre les mains de personnes non autorisées par la loi à les recevoir, les traiter et les exploiter, et ne soient jamais utilisées à des fins incompatibles avec le Pacte. Il serait souhaitable, pour assurer la protection la plus efficace de sa vie privée, que chaque individu ait le droit de déterminer, sous une forme intelligible, si des données personnelles le concernant et, dans l'affirmative, lesquelles, sont stockées dans des fichiers automatiques de données, et à quelles fins. Chaque individu doit également pouvoir déterminer les autorités publiques ou encore les particuliers ou les organismes privés qui ont ou peuvent avoir le contrôle des fichiers le concernant. Si ces fichiers contiennent des données personnelles incorrectes ou qui ont été recueillies ou traitées en violation des dispositions de la loi, chaque individu doit avoir le droit de réclamer leur rectification ou leur suppression* » (§.10) 10°. Mais c'est évidemment dans le cadre européen que les efforts les plus fructueux ont été menés à bien[78]. On peut se demander si les deux pistes de travail qui ont été suivies correspondent à deux étapes ou à deux époques. L'évocation de la législation des Nations Unies nous amene à souligner celle de l'Afrique ?

[77] Résolution 45/95 du 14/12/1990 de l'assemblé générale ONU.
[78] Avec l'avènement de nouveau RGPD.

2. L'Afrique

Au niveau communautaire africain, il s'agit, d'une part, l'acte additionnel A/SA,1/01/10 du 16 février 2010, relatif à la protection des données à caractère personnel dans l'espace CEDEAO et, d'autre part, la Convention de l'Union Africaine sur la sécurité dans le cyber espace et la protection des données à caractère personnel ou Convention de Malabo, du 27 juin 2014 qui constituent les instruments juridiques communautaires. Dans le cadre du continent africain, nous examinerons d'une part la convention de l'Union Africaine(A) et d'autre part l'acte additionnel de la CEDEAO(B)

a. Convention de l'Union Africaine

La Convention de l'Union Africaine sur la sécurité dans le cyber espace et la protection des données à caractère personnel ou Convention de Malabo, du 27 juin 2014, qui requiert la ratification de 15 pays africains pour être effective[79].

L'objet est de protéger les droits des personnes en matière de traitements de données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables de traitement[80].Après un bref aperçu de la convention de UA, il est opportun d'évoquer l'acte additionnel de la CEDEAO.

b. L'acte additionnel A/SA,1/01/10 du 16 février 2010, relatif à la protection des données à caractère personnel dans l'espace CEDEAO

Cet instrument juridique pose les jalons du droit à la protection des données personnelles et invite chaque État à se doter d'une loi et d'une autorité de contrôle.

Pour rappel, l'Acte additionnel A/SA 1/01/10 de la CEDEAO relatif à la protection des données à caractère personnel a été adopté par les Chefs d'État de la CEDEAO en février 2010. . Les sept piliers de l'Acte additionnel sont :

- Définition du cadre juridique de la protection des données à caractère personnel (Définitions de notions essentielles, objet et champ d'application)
- Formalités nécessaires au traitement (déclarations, autorisations, les traitements pour le compte du service public)

[79] Convention de Malabo, du 27 juin 2014.elle n'est pas encore rentrée en vigueur pour de : faut défaut de nombre de ratification.
[80] Dans le même sens que toutes les législations en matière de protection des données personnelle.

- ❖ Cadre institutionnel (autorité administrative indépendante pour garantir le respect des principes et droits consacrés)
- ❖ Principes directeurs (consentement, légitimité, licéité, loyauté, finalité, pertinence, conservation, exactitude, transparence, confidentialité, sécurité, etc.)
- ❖ Principes spécifiques (origine raciale, ethnique, l'état de santé, transfert vers un pays tiers, interconnexion de fichiers, etc.)
- ❖ Droits des personnes fichées (droit à l'information, d'accès, d'opposition, de rectification ou de suppression)
- ❖ Obligations du responsable du traitement (confidentialité, sécurité, conservation et de pérennité)
- ❖ L'Acte additionnel entre en vigueur dès sa publication au Journal Officiel de la Communauté et des États membres. En 2013, six (06) États francophones ont publié l'Acte additionnel sur la protection des données personnelles notamment le Bénin, le Burkina Faso, Cap-Vert, le Ghana, le Niger et le Sénégal.

Paragraphe II : cadre juridique interne

Les dispositions internes relatives à la protection des données à caractère personnel au Burkina Faso est loi n°010 du 20 avril 2004 portant protection des données à caractère personnel. Avant d'effectuer une présentation de LPDP (B) nous dirons un mot sur l'origine de son adoption(A)

A. Origine

C'est à la rencontre de Ouagadougou, à l'occasion de la 9e conférence des chefs d'Etats et de Gouvernements de l'OIF, les 26 et 27 novembre 2004[81], que l'engagement des dirigeants africains d'œuvrer pour une protection des données personnelles de leurs citoyens. Le Burkina Faso a été le premier pays à adopter une loi sur la protection des données personnelles en Afrique. D'autres pays ont suivi la dynamique : Afrique du Sud, Cap-Vert, Bénin, Côte-d'Ivoire, Gabon, Ghana, Guinée Conakry, Niger, Mali, Maroc, Mauritanie, Sénégal, Tchad, Tunisie. Après avoir précisé l'origine de LPDP, nous la présenterons.

[81] C'est la première convention ayant trait à la protection des données en Afrique.

B. La présentation de la loi n°010-2004/AN du 20 avril 2004

La présentation de la LPDP nécessite de définir dans un premier temps ses concepts clés (1) et dans un second d'analyser son champ d'application (2).

1. Définition des concepts clés de la loi

C'est à partir de 2004 que le législateur burkinabè a mis en place les règles particulières à la protection des données à caractère personnel de ses citoyens[82]. Avant cette date, la vie privée était garantie par les règles du droit commun[83] telles que le code du travail, la responsabilité civile, le code Civil, code des personnes et de la famille etc... Cette législation a été élaborée à l'image de la législation française informatique et des libertés (LIL) de 1978 modifiée par loi de 2004[84]. La nouvelle loi a pour objet de protéger au Burkina Faso les droits des personnes en matière de traitement de données à caractère personnel, quels qu'en soient sa nature, le mode d'exécution ou les responsables[85] .

Elle définit les données à caractère personnel comme toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, notamment par référence-à un numéro d'identification ou à plusieurs éléments spécifiques propres à leur identité physique, -psychologique, psychique, économique, culturelle ou sociale[86]. Le RGPD donne une définition satisfaisante de la notion de protection des données à caractère personnel. Selon le règlement, une donnée à caractère personnel est définie comme une information se rapportant à une personne identifiée ou identifiable[87]. De ce fait, avec le nouveau règlement, l'adresse IP est considérée comme étant une donnée personnelle si toute fois il identifie les personnes concernées[88].

Le traitement de données personnelles est défini comme « *toute opération ou ensemble d'opérations effectuées à l'aide de procédés automatisés ou non par une personne physique ou morale, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'extraction, la consultation, l'utilisation ,la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou*

[82]C'est par la loi n°010-2004 /AN du 20 avril 2004 portant protection des données à caractère personnel.
[83] Article 9 et suivant du code Civil du Burkina Faso.
[84]La législation burkinabé tire exclusivement sa source à celle française en faisant naitre en elle-même des insuffisances.
[85] Article 1er de Loi n°010-2004/AN précité.
[86] Dans le même sens qu'article 2 de la nouvelle loi informatique et liberté précité.
[87] RGPD Précité.
[88] L'adresse IP permet de déterminer la personne connectée avec tel ordinateur, à tel endroit et à telle heure.

l'interconnexion ,le verrouillage, l'effacement ou la destruction »[89]. Cette définition appelle deux observations[90]. D'abord le traitement des données dont il est question concerne aussi bien le traitement par recours aux procédés électroniques[91] que les traitements analogiques[92].Ensuite la notion de traitement des données est définie largement et les opérations indiquées ne sont pas exemplatives.

Le responsable de traitement s'entend selon l'article 4, al.1er de la LPDP « ……. *La personne physique ou morale, publique ou privée qui a le pouvoir de décider de la création des données à caractère personnel* ». Cette conception de la notion de responsable de traitement est particulièrement inexacte. En effet selon le Professeur Dominique W. KABRE, ce dernier ne crée pas de données, il n'assure que le traitement et plus exactement, il détermine les finalités et les moyens de ce traitement. La définition de l'acte Additionnel de la CEDEAO est plus éclairante. Son article 1er définit le responsable de traitement comme « *une personne physique ou morale, publique ou privée, tout autre organisme ou association qui seul ou conjointement avec d'autre prend la décision de collecter les données à caractère personnel et en détermine le traitement* ».

La personne concernée est la personne dont les données sont l'objet de traitement[93]. En principe, les personnes concernées par la protection légale sont les personnes physiques. A contrario, les personnes morales se trouvent exclues du champ de cette protection[94]. Selon la législation française, la loi trouvera à s'appliquer s'agissant par exemple des personnes physiques représentants légaux de personnes morales lorsque celles-ci sont nominativement désignées dans un fichier[95].

Le destinataire de traitement est défini comme « *toute personne physique ou morale, publique ou privée, autre que la personne concernée, le responsable de traitement, habilitée à recevoir communication de ces données à caractère personnel* »[96].Ainsi, toute personne qui est habilité à recevoir des données à caractère personnel autre que les personnes suscitées, est appelée destinataire de traitement. Le nouveau règlement de l'Union Européenne prévoit la même définition mais apporte des dérogations. En effet, selon ce règlement, les personnes publiques qui sont susceptibles de recevoir communication de données à caractère personnel

[89] Article 3 de la LPDP et 1er de l'Acte additionnel de la CEDEAO.
[90] D. W. KABRE, Droit des technologies de l'information et de la communication, Burkina Faso, op, cit. P.111.
[91] Signifie support numérique.
[92] Signifie support papier.
[93] Article 4 alinéa 1 LPDP et article 4 de l'Acte additionnel CEDEAO précités.
[94] Cf. nouveau RGPD, la LPDP reste muette en la matière.
[95] Sur les conditions d'applicabilité de la loi aux personnes morales. Voir notamment, CNIL, Délibération n° 84-28 du 3 juillet 1984.
[96] Article 4 al.2 de la LPDP et art.1 de l'acte additionnel de la CEDEAO.

dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre, ne sont pas considérées comme des destinataires[97].Une fois les concepts définis, nous analyserons le champ d'application de la LPDP.

2. Le champ d'application de la LPDP

La notion de données à caractère personnel ayant été déjà définie, il reste à déterminer le champ d'application territoriale de la loi.

Il en va ainsi de l'article 8 relatif au champ d'application de la loi. Selon cet article la présente loi s'applique aux traitements automatisés ou non de données à caractère personnel contenues ou appelées à figurer dans les fichiers. Cela voudrait dire par exemple que la loi n'a vocation à s'appliquer aux traitements automatisés que s'il y a constitution d'un fichier. Pourtant, cela est en déphasage total avec l'ensemble des législations de protection des données qui se sont toujours appliquées aux traitements automatisés de données à caractère personnel en principe. Les traitements non automatisés n'étant concernés que s'il y a constitution de fichiers. Depuis toujours, ce sont les traitements automatisés de données qui ont été perçus comme porteurs de risques pour les personnes. Ainsi, ne soumettre ces traitements à la loi que s'il y a constitution de fichiers revient à mettre en marge la loi de nombreux traitements potentiellement dangereux. Certaines contradictions peuvent aussi être relevées concernant par exemple l'article 11 qui prévoit que la loi ne s'applique pas aux traitements de données ayant pour fin le suivi thérapeutique ou médical des patients alors que par l'application de nombres de dispositions de la loi (articles 17, 20, 21, 23), ces traitements se trouvent cernés par la loi. Enfin certaines formulations s'avèrent maladroites entraînant une incertitude sur le contenu de la loi. A la lecture de l'article 14, par exemple, on peut se poser la question de savoir si la réutilisation des données est-elle admise ou non. En effet, si l'alinéa premier prévoit que les données ne peuvent être utilisées qu'en vue des finalités pour lesquelles elles ont été collectées, ce qui exclut à priori toute réutilisation. L'alinéa 2 semble admettre cette réutilisation en prévoyant la proportionnalité des données «au regard des finalités pour lesquelles elles sont traitées ultérieurement ».

Le même article 8 de la LPDP précise que celle-ci s'applique aux traitements automatisés ou non de données à caractère personnel des responsables de traitement établi sur le territoire du Burkina Faso, ou, sans y être établi, recourt à des moyens de traitement situés

sur le territoire du Burkina Faso, à l'exclusion des données qui ne sont utilisées qu'à des fins de transit. Il relève de cette disposition que LPDP s'applique aux traitements de données automatisées telles que les fichiers informatisés de données ou non automatisés tels que les fichiers de données sur support papier réalisé par des responsables établis au Burkina Faso ou qui, sans y être disposent au Burkina Faso des moyens de traitement des données personnelles. Cette discussion suscite des interrogations[98]. En effet, si la première hypothèse ne pose pas de difficultés, il en va tout autrement de la seconde. Que faut-il entendre par recours aux moyens de traitements situés au Burkina Faso ? Il peut s'agir d'une entreprise établie à l'étranger mais qui dispose au Burkina Faso des moyens de collecte des données à caractère personnel[99].

Après l'élaboration du cadre juridique, il nous est judicieux d'évoquer les conditions de traitement des données dans la section II.

Section II : Les conditions de traitement des données à caractère personnel

Le traitement des données à caractère personnel doit nécessairement obéir à des conditions définies par les règles de protection des données personnelles. Pour cela, nous consacrons dans le paragraphe I les principes directeurs d'utilisation légitime des données à caractère personnel et dans le paragraphe II les droits des personnes concernées ainsi que les obligations des responsables du traitement des données à caractère personnel.

Paragraphe I : Les principes directeurs d'utilisation légitime des données à caractère personnel

La législation en matière de protection des données personnelles prévoit un certain nombre de principes tels que le principe de consentement préalable(A), le principe de loyauté et de licéité(B), le principe de qualité des données(C), le principe de finalité de traitement(D) et le principe de confidentialité et de sécurité(E).Nous évoquerons successivement ces principes .

A. Le principe de consentement préalable

Selon le législateur burkinabè, tout traitement des données à caractère personnel effectué doit avoir reçu le consentement des personnes concernées sauf dérogation prévue par

[98] D. W. KABRE, Droit des technologies de l'information et de la communication, Burkina Faso, op., cit., P.11.
[99] C'est le cas des GAFAM.

la loi[100].Le législateur ne définit pas le consentement. Il se contente de dire que consentement doit être libre, éclairé et informé. Le consentement peut être défini comme l'expression d'une manifestation de volonté. En droit, il revêt une fonction particulière, en ce qu'une personne, par son consentement, pourrait accepter une situation juridique susceptible de lui causer un préjudice. Notion fondamentale dans la pensée juridique, le consentement est omniprésent, que ce soit, par exemple, en droit pénal, lorsqu'il conditionne l'interprétation d'une situation litigieuse comme licite ou illicite, ou en droit des contrats, dans lequel il constitue une des conditions essentielles de validité de l'acte établi entre les parties[101] La dérogation est possible dans le cas où le traitement des données est nécessaire[102] :

- Au respect d'une obligation légale à laquelle le responsable de traitement est soumis ;
- A l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité ; publique dont est investi le responsable de traitement auquel les données sont communiquées ;
- A l'exécution d'un contrat auquel la personne concernée est partie ou l'exécution de mesures précontractuelles prises à sa demande ;
- A la sauvegarde de l'intérêt ou des droits et libertés fondamentaux du client.

Le consentement est aujourd'hui érigé en condition de licéité des traitements de données à caractère personnel dans la quasi-totalité des législations de protection des données[103]. Il figure parmi « *un noyau dur* » de principes, auxquels des dérogations ne sont apportées qu'à titre exceptionnel[104]. L'importance qui s'attache au consentement est à mettre en relation avec le rôle de plus en plus important qui est reconnu aujourd'hui à la personne qui doit être considérée comme étant à même de décider pour elle-même. On lui reconnaît, en ce sens, un droit à l'autodétermination informationnelle. En matière de consentement, un des reproches adressés à la LPDP est de ne pas expliquer davantage ce que l'on entendait par un consentement libre, éclairé et informé. Le consentement de la personne concernée ne suffit pas, il faut que le traitement des données soit loyal et licite.

[100] Article 5 de la LPDP.
[101] Article 1108 du code civil précité.
[102] Article 23 de l'acte additionnel CEDEAO précité.
[103] Ancienne directive 95/46/CE, dans son article 2 (h) ; Article 1108 du Code civil belge.65Art. 2, h), de la Directive 95/46/CE.66Art. 7, de la Directive 95/46/CE ; 67Art. 8 de la Directive 95/46/CE.68Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement du 13 juillet 2011, p.28.
[104] Idem.

B. Principe de loyauté et de licéité

Conformément à l'acte additionnel de la CEDEAO sur la protection des données personnelles, les données doivent être collectées et traitées de manière loyale, licite et non frauduleuse[105]. La licéité de traitement signifie que ce dernier doit respecter toutes les règles légales de la protection. La loyauté de traitement suppose que la collecte et le traitement doivent se faire dans la transparence, c'est à dire que l'utilisation doit respecter la destination du traitement qui est l'exécution du contrat[106]. En outre, la personne concernée doit être informée de la finalité du traitement, de l'identité des responsables de traitement et des destinataires éventuelles des données collectées. L'absence de fraude est une conséquence du principe de loyauté et exige du responsable de traitement de décliner le but réel et les moyens de traitement[107]. Le respect de ce principe exige également l'observation du principe de qualité des données.

C. Les principes de qualité des données.

Les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités des traitements[108]. Cela signifie que les données doivent être non seulement utiles pour un traitement mais aussi nécessaire, ce qui implique qu'une donnée ne peut être conservée et traitée que s'il n'existe pas un autre moyen moins dommageable pour les libertés individuelles[109].

L'exigence que les données ne soient pas excessives implique que les données ne doivent pas être traitées si ces dernières causent une atteinte disproportionnée à la vie privée des personnes concernées.

De nombreux principes de qualité des données doivent être respectés lorsqu'on traite de données sur les espèces particulièrement en ce qui concerne l'aspect spatial de ces données[36]. Ces principes doivent être appliqués à toutes les étapes du processus de gestion des données (saisie, numérisation, stockage, analyse, présentation et utilisation). Il y'a deux clés pour améliorer la qualité des données : la prévention et la correction.

[105] Article 24 Acte CEDEAO et ARTICLE 12de LPDP.
[106] D. W. KABRE, Droit des technologies de l'information et de la communication, Burkina Faso, op. cit. , p. 115.
[107] Idem.
[108] Article 25 Acte CEDEAO et 14 de la LPDP.
[109] La liberté individuelle doit un principe fondamental garantie par toutes les législations.

La prévention des erreurs est étroitement liée à la fois à la collecte des données et à la saisie des données dans la base. La correction des erreurs joue, cependant, un rôle particulièrement important dans le cas des collections patrimoniales qui fournissent un grand nombre des données primaires sur les espèces et des données. Cependant, il est important que les personnes concernées développent une vision et une politique de la qualité de leurs données[110].

La LPDP et l'acte additionnel de la CEDEAO prévoient l'exactitude des données[111.] Ainsi, si les données sont incomplètes ou inexactes, elles peuvent faire l'objet de correction ou de rectification. La Loi Informatique et Liberté et le RGPD vont au-delà de la rectification en consacrant le droit à l'oubli ou droit à l'effacement qui permet à la personne concernée d'exiger l'effacement de ses données personnelles.

Les données doivent être conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités de traitement pour lesquelles elles sont collectées ou traitées [112].Selon le professeur Dominique W. KABRE, cette disposition semble consacrer ce que la doctrine a qualifié de droit de l'oubli[113].Il est cependant possible de conserver les données au-delà de la durée nécessaire sous forme anonyme ou sous forme nominative à des fins historiques, statistiques ou de recherche. Après avoir évoqué le principe de qualité des données, il nous a fallu souligner le principe de finalité de traitement des données.

D. Principe de finalité de traitement des données

Tout comme la loi française, la loi burkinabé du 20 avril 2004 sur la protection des données à caractère personnel pose le principe de la légitimité de la finalité de tout traitement de données à caractère personnel. Selon l'article 14 de la loi, « *les données doivent être collectées pour des finalités déterminées, explicites et légitimes* »[114].

[110] Cette prérogative est reconnue aux personnes concernées d'accéder à leurs données puis rectifier ou les effacer.
[111] Article 17 de la LPDP et article 26 de l'Acte CEDEAO.
[112] Article 14 LPDP et 25 Acte Additionnel.
[113] Lorsque les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, ce qu'on appelle droit à l'oubli ,article 17-1 du RGPD précité.
[114] De même l'article 5 al.1-b du règlement.

En conséquence, les données ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été collectées[115].

C'est le principe essentiel de la protection des données. C'est le but dans lequel ces données doivent être collectées qui peut mettre en mal la vie privée du client[116]. Pour fondamental qu'il soit, le principe de finalité n'est toutefois pas défini légalement. Selon I. de Lamberterie, «*la finalité constitue la raison d'être d'un traitement particulier de données personnelles. Elle est l'objectif désigné lors de la constitution d'un traitement dont elle commande la création. A ce titre, elle justifie les caractéristiques maîtresses du traitement (qualité des données, durée ...)* »[117] . On retrouve cette même idée chez Mme Claire Marliac-Négrier pour qui, «*la finalité d'un traitement se définit comme étant le but envisagé, son objet. Le traitement sera de la sorte limitée à sa finalité et la collecte des informations sera elle-même cantonnée au strict nécessaire en fonction de la finalité* »[118] Déterminer la finalité du traitement suppose expliciter ses objectifs, les raisons d'être de sa mise en œuvre. La finalité doit être explicite et déterminée pour l'exécution du contrat. La finalité de traitement des données doit être légitime, c'est à dire utile et nécessaire au vu de l'objet social de l'entreprise et de l'intérêt général[119]. Les traitements doivent être compatibles avec les finalités, c'est à dire que les données ne peuvent être utilisées à des fins que celles pour lesquelles elles ont été collectées. En Europe, Le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement[120].Le législateur burkinabé est muet dans en ce sens. Dans ce cas, aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise. Outre ces principes, les responsables de traitement doivent obéir au principe de confidentialité et de sécurité.

[115] Selon le nouveau règlement, le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales.

[116] D.W. KABRE, Droit des technologies de l'information et de la communication, op.,cit., p. 115.

[117] I. de Lamberterie, H.-J. Lucas (dir.), Informatique, libertés et recherche médicale, op.,cit., p. 79. n° 199

[118] C. Marliac-Négrier, La protection des données nominatives informatiques en matière de recherche médicale,op.,cit., p 10.

[119] D. W. KABRE, droit des technologies de l'information et de la communication, op.,cit., p.116.

[120] Article, précité, nouveau RGPD.

E. Principe de la confidentialité et de sécurité

Les données personnelles doivent être traitées de manière confidentielle et protégées contre toute destruction accidentelle, perte ou toute divulgation non autorisée[121].Le RGPD va jusqu'à proposer des pistes de mesures de sécurité à prendre telles que la pseudonymisation des données personnelles afin qu'elles deviennent non identifiables[122].Ces mesures amoindrissent les inquiétudes des individus concernant l'exploitation des données auxquelles elles ont consenti. Malheureusement, la pseudonymisation comporte des limites. Sa prétendue vertu de désidentification des données est souvent remise en cause par de nombreuses recherches. Après avoir élaboré les différents principes directeurs relatifs à la protection des données personnelles, il nous est judicieux d'évoquer les droits des personnes concernées et les obligations des responsables du traitement des données à caractère personnel. Après avoir évoqué les principes directeurs du traitement légitime des données personnes, il est opportun de préciser les droits des personnes concernées et les obligations des responsables du traitement des données personnelles.

Paragraphe II : Les droits des personnes concernées et les obligations des responsables du traitement des données à caractère personnel

Nous évoquerons dans ce paragraphe les droits (A) et les obligations des personnes concernées(B).

A. Les droits des personnes concernées par le traitement

Pour permettre à la personne concernée de jouer un rôle actif dans la protection de ses données personnelles, les règles de la protection des données personnelles lui accordent un certain nombre de droits.

[121] Article 28 Acte CEDEAO et 15 LPDP.

[122]L'article 4, § 5, du Règlement définit la pseudonymisation comme «le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable»

1. Droit à l'information

Le responsable de traitement[123] de données à caractère personnel a l'obligation d'informer la personne concernée de son identité ou celle de son représentant, de la finalité du traitement, des catégories de données traitées, des destinataires des données de ses droits d'accès et de rectification, de la durée de la conservation, du transfert éventuel des données vers l'étranger[124].Dans la pratique au Burkina Faso, les entreprises évoluant dans les technologies ne déterminent pas au préalable la durée de la conservation des données personnelles pendant la collecte de ces données personnelles, ce qui est de nature à entrainer des réutilisations abusives non prévues dans le contrat[125]. Cette pratique est un manquement à la législation en la matière en raison de la complexité et de l'insuffisance de la LPDP qui ne fixe pas un délai de prescription pour leur conservation par le responsable de traitement[126].

Le nouveau RGPD est plus claire. En effet, il dispose dans son article 14 al1.d que la personne concernée peut lorsque le droit d'accès est possible, intervenir pour discuter avec le responsable si la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée, ce qui n'est pas le cas en droit burkinabè. En France, la loi informatique et des libertés[127] prévoit une durée de conservation définie et limitée. En effet la durée de conservation doit être définie par le responsable du fichier, sauf si un texte impose une durée précise. Cette durée va dépendre de la nature des données et des objectifs poursuivis. Exemples de durées de conservation[128] **:**

Par exemple, lors d'un achat sur internet, les coordonnées de la carte bancaire du client ne peuvent être conservées que le temps de réalisation de l'opération de paiement. Ainsi, au terme de la réalisation de cet objectif (l'achat du bien dans l'exemple précédent), les données doivent être :

- Effacées ou ;
- Archivées (voir ci-dessous) où ;
- Faire l'objet d'un processus d'anonymisation des données, afin de rendre impossible la « *réidentification* » des personnes. Ces données, n'étant plus des données à caractère personnel, peuvent ainsi être conservées librement et valorisées notamment par la

[123] Prédéfini.
[124] Article de la LPDP et article 12 al.1 du RGPD.
[125] Ce que nous avons constaté au moment de nos entretiens avec les responsables de ces entreprises.
[126] Le nouveau règlement n'a pas défini de délai fixe à la conservation des données mais se réserve de dire que ces données peuvent être conservées autant qu'elles sont nécessaires à la finalité des traitements. Il en est ainsi pour des finalités ultérieures compatibles à la finalité initiale. La législation burkinabé manque de précision.
[127] Loi informatique et liberté précité.
[128]www.cnil.fr limiter la conservation des données, consulté le « 02/01/2019 à 12H 30 ».

production de statistiques. 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...).En plu du doit d'information, les personnes concernées bénéficient d'un droit d'accès.

2. Droit d'accès

Le droit d'accès est prévu par l'article 17 alinéa 1 de la LPDP.Il donne la possibilité aux personnes concernées « *de connaître les données conservées qui les concernent* ». Ce droit doit être effectif en devant s'exercer sans délai ou frais excessifs. Cependant, l'effectivité du droit d'accès pourra être limitée dans la mesure où la loi ne prévoit consécutivement aucun droit à la communication des données. En l'absence d'un tel droit, on peut s'interroger sur le sens d'un droit d'accès. En quoi consisterait-il ? Sans doute, implicitement, le droit d'accès ici reconnu s'entend aussi d'un droit d'obtenir une copie des données. De même, le texte de loi ne précise que les données communiquées doivent l'être sous une forme compréhensible pour les personnes concernées. On pourra également considérer ici que cette exigence est implicitement contenue dans l'alinéa 1er de l'article 17. Cependant, une précision formelle n'est pas inutile.

Concernant les données médicales, le droit d'accès s'exerce par l'intermédiaire d'un médecin désigné par la personne concernée[129]. On rappellera la contradiction de cette disposition avec l'article 11 qui prévoit que sont exclus du champ d'application de la loi sur le traitement de données ayant pour finalités le suivi thérapeutique ou médical individuel des patients[130]. La législation burkinabè n'est pas claire sur l'exercice du droit d'accès en raison du fait qu'elle ne précise pas le but du droit d'accès par la personne concernée de façon explicite. Contrairement à la LPDP, nouveau RGPD définit l'objectif du droit d'accès et prévoit des dispositions plus protectrices des droits des personnes concernées. Son article 15 alinéa 1 dispose que *« la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que quelques informations prévues aux paragraphes a à h .En son alinéa 2 le responsable du traitement*

[129] Article 17 alinéa 2.
[130] La LPDP est ambiguë dans ce cas. Si la LPDP ne s'applique pas aux données médicales, il n'y a pas de raison qu'elle détermine les conditions d'accès aux données médicales.

fournit une copie des données à caractère personnel faisant l'objet d'un traitement ». Le législateur burkinabè doit revoir et élargir les différentes prérogatives de cette disposition qui permet aux personnes concernées d'exercer directement leur droit sur la protection de la vie privée »[131]. Après avoir analysé le droit d'accès, nous allons nous intéresser au droit de rectification des personnes concernées.

3. Droit de rectification

Si un droit de rectification existe, sa portée est toutefois limitée par rapport aux dispositions de la loi française. Alors que le texte français étend la rectification aux données inexactes, incomplètes, équivoques, périmées ou le traitement est interdite, l'article 17 alinéa 3 de la LPDP le limite aux cas où les données seraient incomplètes ou inexactes. Sans doute, le caractère inexact des données peut-il être largement entendu en recouvrant des hypothèses comme le caractère équivoque ou périmé des données mais il ne semble pas devoir couvrir l'hypothèse de données dont le traitement est interdit. En ce sens, le droit de rectification pourrait être complété.

Il permet à la personne concernée d'obtenir la rectification ou la correction des données incomplètes ou inexactes la concernant. Il s'exerce à l'égard du responsable du traitement qui doit procéder à la correction ou à la rectification et délivrer une copie à la personne concernée de l'enregistrement concernant la modification. Si le traitement intéresse la sureté de l'Etat, la défense et la sécurité sociale, la demande doit être adressée à la Commission de L'informatique et des Libertés chargé de désigner un de ses membres pour le droit d'accès et de rectification[132]. Les vérifications et corrections effectuées sont ensuite portés à la connaissance du requérant.

L'évocation du droit de rectification nous oblige à analyser le droit d'opposition des personnes concernées.

4. Droit d'opposition

Il permet à la personne de s'opposer au traitement des données à caractère personnel en invoquant des raisons légitimes. C'est le cas où le responsable de traitement ne respecte pas les

[131] La LPDP a intérêt à évoluer dans le sens du RGPD.
[132] D. W. KABRE, Droit des technologies de l'information et de la communication,op.,cit ., p. 122.

principes de qualités des données[133].Il appartient à la personne concernée de faire la preuve des circonstances et des motifs légitimes[134].

L'article 21 du RGPD prévoit que la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière à un traitement des données à caractère personnel la concernant, y compris un profilage fondé sur ces dispositions.

Dans le même sens, l'article 38 de la LIL révisé dispose que toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Il ressort de ces 3 dispositions qu'il existe un vrai droit pour la personne concernée de s'opposer au traitement de ses données à caractère personnel[135].

Cette faculté qui lui est conférée n'est, cependant, pas sans limite, le droit d'opposition n'étant pas discrétionnaire. Tant le RGPD, LPDP que la loi informatique et libertés assortissent le droit d'opposition de limites.

Tandis que la LIL et LPDP subordonnent le droit d'opposition par la personne concernée à l'existence de « *motifs légitimes* », le RGPD exige que son exercice soit justifié par « *des raisons tenant à sa situation particulière* ».

De toute évidence, la notion de « *situation particulière* » est plus large que celle de « *motifs légitimes* ».

Les conditions d'exercice du droit d'opposition posées par le RGPD sont, de la sorte, moins restrictives. S'agissant de la notion de « *motifs légitimes* », il n'est pas inintéressant de relever que dans un arrêt du 28 septembre 2004, la Cour de cassation avait considéré qu'en matière politique, philosophique ou religieuse, la condition de l'existence de motifs légitimes « *est remplie par le seul exercice de la faculté, pour la personne concernée, de s'opposer au traitement de données personnelles* »[136][137]

C'est donc une appréciation extrêmement large de la notion qui est faite par la Cour de cassation.

En vertu du caractère discrétionnaire prévu, L'article 21, 2 du RGPD prévoit que lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la

[133] La qualité de données renvoie à la conservation des données inutiles, inexactes, non pertinente ou adéquates.
[134] D. W. KABRE, Droit des technologies de l'information et de la communication, op. cit., P.123.
[135] Toutes ces législations protègent la personne concernée par le biais de l'exercice de son droit d'opposition.
[136](Cass. Crim., 28 sept. 2004, n° 03-86.604).

[137] (https://aurelienbamde.com/2018/12/23/rgpd-le-droit-dopposition/ consulté le 12 février à 15H 24.

concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.

Une fois les droits des personnes concernées évoqués, nous allons nous intéresser aux obligations des responsables du traitement.

B. Les obligations du responsable du traitement

La LPDP fait naitre à la charge des personnes responsables plusieurs obligations dont il est judicieux d'évoquer dans les points ultérieurs.

1. L'obligation d'information

Le responsable du traitement doit informer la personne concernée de la finalité, des destinataires des données, du caractère obligatoire ou facultatif des réponses aux questions[138].

Outre l'obligation d'information, une obligation de confidentialité et de sécurité est à la charge des responsables du traitement.

2. L'obligation de confidentialité et de sécurité des données

Elle impose au responsable de traitement de prendre toutes les mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou accès non autorisée[139]. S'agissant des mesures techniques , il s'agit des mesures de sécurité physique (protection contre la destruction physique, l'incendie, le gel, les pannes d'électricité…) et des mesures de sécurité logique(protection contre l'accès et la modification du système informatique).Ces mesures doivent permettre de respecter les principes de traitement et de qualité des données .S'agissant des mesures organisationnelles, celles-ci englobent toutes les mesures qui doivent tendre à conscientiser le personnel au problème de la sécurité et au respect de la législation relative à la protection des données personnelles . Ces mesures doivent être proportionnées aux risques encourus et être adéquates au regard de l'art et de la technique[140].

[138] Article 14 LPDP.
[139] Article 15 de la LPDP.
[140] D.W. KABRE, Droit des technologies de l'information et de la communication, op.cit., p. 124.

Certaines entreprises de technologies ont mis en place plusieurs mesures techniques et organisationnelles telles que les politiques de sécurité des données, la charte de gestions des risques et la matrice des risques[141].

Nous avons constaté dans la société MTOPO PAYMENT SOLUTIONS BF que toutes ces mesures ont été mise en place dans le cadre de la protection des données personnelles, les données anonymisées sur les logiciels et dans les équipements informatiques.

Selon MTOPO payement solutions BF[142], l'objectif de la politique de la sécurité vise à atteindre la réalisation des 3 composants de base de la sécurité : la confidentialité, l'intégrité et la disponibilité[143]. La confidentialité est le caractère réservé d'une information dont l'accès et la diffusion sont limités aux seules personnes autorisées à la connaître. L'intégrité est la protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci. La disponibilité est l'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

Dans la procédure de matrice des risques, MTOPO en tant qu'agrégateur des paiements, se donne les moyens organisationnels, techniques et opérationnels pour non seulement comprendre et identifier les risques, mais aussi et surtout pour prendre les mesures idoines pour mettre ceux-ci sous contrôle[144].

Le risque est un événement dont la survenance n'est pas certaine mais entraîne pour la personne fichée un dommage[145]. Dans cette industrie comme dans d'autres évoluent ; identifier les risques n'est donc pas un exercice statique. C'est plutôt un exercice continu qui doit être mis en œuvre méthodiquement et rigoureusement.

Ce document décrit les risques identifiés par la société en ce début de ses activités ; et ceci est une base sur les pratiques de l'industrie de paiement et les cadres de références associés. Il présente aussi les mesures de mitigation mises en œuvre pour cela.

La charte de la gestion des risques est mise en place pour définir le but, les valeurs, les objectifs, le domaine d'action, les responsabilités, l'autorité et le statut de la gestion des risques. Elle vise à offrir aux acteurs de la gestion des risques, une compréhension claire de leurs rôles respectifs dans le domaine de la gestion des risques[146]. Cette charte fera l'objet d'une revue

[141] Nous l'avons constaté lors de notre stage à MTOPO PAYMENT SOLUTIONS BF en 2018-2019.
[142] MTOPO PAYEMENT SOLUTIONS BF, SARL à capital de 10.000 000 fcfa.
[143] Cf. politique de sécurité de MTOPO 2019, p.2.
[144]Cf. Procédure de matrice MTOPO 2019 ; p.3.
[145] Pr Yves Poulet, « protection des données personnelles et obligation de sécurité », p. 19.
[146] Cf. Charte de la gestion des risques MTOPO PAYMENT SOLUTIONS BF 2019, p. 3.

annuelle par le département de la gestion des risques et sera approuvée par le président du Comité des Risques.

Ces mesures organisationnelles mises en place permettent une meilleure protection des données à caractère personnel au sein de l'entreprise et dans les logiciels mise à la disposition à ses clients.

L'analyse de l'obligation de confidentialité et de sécurité, nous oblige à évoquer celle de notification.

3. L'obligation de notification

Cette obligation exige tout responsable de traitement de faire une déclaration de tels traitements des données auprès de la Commission Informatique et des Libertés[147]. Cette déclaration doit indiquer un certain nombre d'informations telles que l'indication[148]:

a) la personne qui présente la demande et celle qui a le pouvoir de décider de la création du traitement de données[149] ou, si elle réside à l'étranger, son représentant au Burkina Faso ;
b) les caractéristiques, la finalité et s'il y a lieu, la dénomination du traitement de données ;
c) le service ou les services chargés de mettre en œuvre celui-ci ;
d) le service auprès duquel s'exerce le droit d'accès ainsi que les mesures prises pour faciliter l'exercice de ce droit ;
e) les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées.

Lorsque les traitements automatisés de données à caractère personnel sont opérés pour le compte de l'Etat, d'un Etablissement public, d'une collectivité territoriale ou d'une personne de droit privé gérant un service public, il doit être décidé par décret pris après avis de la CIL[150].

Cette obligation doit être exécutée par le responsable de traitement avant la mise en œuvre de traitement des données personnelles au Burkina. C'est une formalité préalable au

[147] Article 19 de LPDP.
[148] Article 42 de la LPDP et l'article 6 de l'acte additionnel CEDEAO.
[149] Cet alinéa de l'article défini mal le responsable de traitement des données personnelles. Celui-ci ne crée pas des données, il traite des données.
[150] Article 18 alinéa 1 de LPDP.

traitement des données personnelles. Au Burkina Faso cette procédure est battue en brèche en raison du fait que bon nombre d'entreprises ne la respectent qu'après le contrôle et la recommandation faits par l'autorité de contrôle (CIL)[151]. En 2010, la CIL a procédé à sa première vérification sur place conformément à l'article 37 de la LPDP auprès de plusieurs secteurs tels que le secteur d'identification Nationale (Office Nationale d'Identification), le secteur politique (Commission Electorale Nationale Indépendante), le secteur de téléphonie (Office Nationale de Télécommunication, TELECEL, ORANGE (ZEN à l'époque)) et le secteur cyber café et autres centres communication internet au Burkina Faso[152]. Au terme de ces missions, la CIL a constaté que ces secteurs n'ont pas accompli leur obligation de déclaration à la CIL, qu'en plus le droit au respect de la sécurité des données n'est pas respecté par ces secteurs d'activités[153]. Elle a ainsi formulé des recommandations portant sur l'obligation de déclaration des traitements des données à caractère personnel à la CIL, de sécurité dans le processus de traitement, le respect de principe de consentement préalable et de finalité des traitements, le principe de conservation limité des données personnelles, le principe de confidentialité, de sécurité des données personnelles , définitions des chartes de bonne utilisation des ordinateurs et de manière générale le respect des droits des personnes concernées par le traitement[154]. Ces responsables de traitement des données devraient se conformer à la LPDP dès son adoption en 2004. Cette violation tire sa source des faiblesses et des insuffisances de la CIL depuis sa création par le décret[155].

En Europe, le régime de déclaration à la CNIL est aboli par le nouveau règlement et est remplacé par la déclaration au registre interne. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tient un registre des activités de traitement effectué sous leur responsabilité[156]. Ce registre comporte toutes les informations relatives aux données traitées, leurs destinataires… (Art 30 du règlement). Ce mécanisme serait bénéfique au Burkina Faso puisqu'il permet à la CIL de procéder au contrôle régulièrement afin de vérifier la conformité des traitements à la loi. Dans la pratique, la CIL après la déclaration et son contrôle à posteriori immédiat à la déclaration n'effectue aucun effort, elle se borne à attendre des plaintes auprès des personnes concernées avant de réagir à lors que ce dernier ignore souvent leurs droits. Ce qui est encore un obstacle à l'évolution de la jurisprudence en matière de traitement des données personnelles au Burkina Faso contrairement aux pays occidentaux.

[151] Rapport public, CIL ,2010.
[152] Rapport public, CIL 2010, P. 12.
[153] Idem p. 13 ;14 ;15 et 16.
[154] Idem.
[155] Dès sa création en 2004, c'est à partir de 2008 que la CIL a été réellement institué.
[156] Ce mécanisme devrait être une leçon pour le Burkina dans la modification de la LPDP.

L'analyse de l'obligation de notification, nous amène à nous intéresser celle de demander une autorisation de traitement.

4. L'obligation de demander une autorisation de traitement

Certains types de données impliquent qu'une autorisation soit donnée par l'autorité de contrôle avant le traitement[157] : il s'agit

- des données génétiques et sur la recherche dans le domaine de la santé ;
- les données relatives aux infractions, condamnation ou mesure de sureté ;
- des données qui font l'objet d'une interconnexion ;
- les données constituées par le numéro national d'identification ou tout autre identifiant de même nature ;
- les données biométriques et les données ayant un motif d'intérêt public notamment à des fins historiques ou scientifiques.

En Europe le nouveau règlement prévoit un allègement des obligations en matière de formalités préalables. La logique de formalités préalables laisse la place à celle de responsabilisation des acteurs. Cet allègement a eu un impact pour le secteur de santé[158]. Pour les traitements suivants comportant des données de santé, les formalités à accomplir auprès de la CNIL disparaissent à certaines conditions :

- Les traitements pour lesquels la personne concernée a donné son consentement exprès ;
- Les traitements nécessaires à la sauvegarde de la vie humaine ;
- Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;
- Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel (ex : dossier médical ou logiciel de gestion médico-administratif, télémédecine, PACS utilisé dans le domaine de l'imagerie médicale, etc.) ;
- Les traitements permettant d'effectuer des recherches à partir des données réalisées par le personnel assurant ce suivi, et destinées à leur usage exclusif (recherche « *interne* ») ;

[157] Article 12 de l'Acte Additionnel CEDEAO.
[158] https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel consulté le « 23 02 2019 à 14h ».

- Les traitements mis en œuvre aux fins d'assurer le service des prestations ou le contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;
- Les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans le cadre du PMSI local ;
- Les traitements effectués par les agences régionales de santé, par l'État et par la personne publique qu'il désigne en application du premier alinéa de l'article L. 6113-8 du code de la santé publique et dans le cadre défini au même article ;
- Les traitements de données dans le domaine de la santé mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la CNIL, ayant pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites.

Outres ces obligations, les responsables du traitement doit obéir aux obligations de perenité.

5. L'obligation de pérennité

Cette obligation impose aux responsables du traitement de veiller à ce que les données personnelles traitées soient exploitables quel que soit le support utilisé[159]. Pour ce faire, il doit assurer l'évolution de la technologie[160].

Après avoir élaboré les différents droits des personnes concernées et les obligations des responsables du traitement, il nous est opportun d'évoquer le contrôle des traitements exercé par la commission.

Section II : Le contrôle des traitements des données

Le contrôle des traitements des données est assuré par une autorité de contrôle ou de protection dénommée Commission Informatique et des Libertés selon l'Acte Additionnel de la CEDEAO portant protection des données à caractère personnel.

La commission est chargée de veiller au respect des dispositions de la loi, notamment en informant toute personne concernée de leurs droits et obligations et en contrôlant les

[159] Article 45 de l'Acte Additionnel CEDEAO.
[160] D. W. KABRE, Droit des technologies de l'information et de la communication, op. cit., p.125.

applications de l'informatique aux traitements des données d'utilisateurs à caractère personnel[161].

La CIL a pour attribution de veiller à ce que le traitement automatisé ou non, public ou privé, d'information nominative soient effectuées conformément à la disposition légale. Elle dispose d'un pouvoir de sanction[162].

Nous évoquerons dans le paragraphe I le contrôle à priori de la mise en œuvre des traitements et dans le paragraphe II le contrôle à posteriori de la mise en œuvre des traitements.

Paragraphe I : Le contrôle a priori de la mise en œuvre des traitements des données à caractère personnel

Fondamentalement, la collecte des données est l'étape préalable indispensable à la mise en œuvre de tout traitement de données à caractère personnel. C'est à travers cette étape que le responsable du traitement accède aux données nécessaires au traitement.

Cette phase du traitement des données doit faire l'objet de toutes les attentions. Ces attentions vont, d'ailleurs, dans un double sens. Il s'agit, d'une part, de garantir la qualité scientifique des traitements au titre desquelles les données concernant les personnes ont vocation à être collectées et traitées et, d'autre part, de respecter des conditions juridiques exigées pour accéder aux données. Toutes les informations personnelles n'étant pas librement accessibles, il convient d'en respecter les conditions juridiques de disponibilité.

Le contrôle à priori s'exerce par l'accomplissement des formalités préalables (déclarations, autorisations et avis) à la mise en œuvre des traitements qu'il convient à évoquer.

A. Les déclarations à la CIL

Conformément à la LPDP toute personne physique ou morale décidant de la collecte des données personnelles a l'obligation de faire la déclaration des traitements à la CIL avant la mise en œuvre des traitements. Cette demande est fondée sur les articles 19 et suivants de la loi sur la protection des données personnelles. En effet, cet article fait obligation aux responsables de traitement de procéder à une déclaration préalable de traitement de données à caractère personnel auprès de l'autorité de protection des données à caractère personnel. A l'instar du Burkina Faso, le Gabon, le Sénégal, respectivement aux articles 51 et suivants de la loi n° 001-

[161] Article 37 LPDP.
[162] CIL, rapport public, 2012.

2011 du 25 septembre 2011, aux articles 18 et suivants de la loi n° 2008-12 du 15 janvier 2008 relative à la protection des données à caractère personnel et aux article 5 et suivant de la loi ivoirienne portant protection des données à caractère personnel ont adopté les mêmes dispositions.

La déclaration consiste à renseigner, une fiche de déclaration téléchargeable sur le site de la commission et la déposer auprès des services de la commission contre récépissé. La déclaration est une formalité plus simple à accomplir contrairement à la rigueur de la demande d'avis et devrait inciter les responsables à la respecter avec célérité. En somme la formalité préalable vise à permettre à l'autorité compétente de connaitre l'identité du responsable du traitement et du type de traitement envisagé en vue de s'assurer du respect de la législation en matière de protection des données à caractère personnel à l'égard des citoyens. C'est pendant cette phase que la CIL autorise et limite les finalités des traitements. La conséquence directe de la limitation a priori de la finalité du traitement est l'interdiction d'utiliser les données suivant une finalité ultérieure qui serait incompatible avec la finalité initiale.

En Europe, avec l'avènement du nouveau RGPD, cette formalité préalable est battue en brèche. En effet, elle est remplacée par la déclaration au registre interne. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité.

Apres l'analyse des déclarations à la Commission, nous nous intéresserons aux demandes d'avis et d'autorisation.

B. Les demandes d'avis et d'autorisation

La demande d'avis est requise pour le compte de l'Etat ou de ses démembrements ou d'une personne morale du droit privé exerçant des services publics aux termes de l'article 18 de la loi précitée. Il ressort que tout traitement effectué dans le cadre de la mission de service public, au compte de service public qu'il soit l'œuvre de l'administration publique ou d'un privé est soumis à l'autorisation de l'autorité compétente. La commission rend un avis motivé. Si l'avis est favorable, le traitement est alors autorisé par un acte règlementaire avant sa mise en œuvre. A contrario si l'avis est défavorable le requérant peut introduire un recours au Conseil d'Etat. A contrario si l'avis est défavorable le requérant peut introduire un recours au Conseil d'Etat.

Certains types de données impliquent qu'une autorisation soit donnée par l'autorité de contrôle avant le traitement[163] : il s'agit

- des données génétiques et sur la recherche dans le domaine de la santé ;
- les données relatives aux infractions, condamnation ou mesure de sureté ;
- des données qui font l'objet d'une interconnexion ;
- les données constituées par le numéro national d'identification ou tout autre identifiant de même nature ;
- les données biométriques et les données ayant un motif d'intérêt public notamment à des fins historiques ou scientifiques.

Beaucoup d'entreprises nationales refusent d'accomplir les formalités préalables à la mise en œuvre des traitements des données[164]. Cela s'explique par le fait que la CIL n'effectue bien pas ses missions de contrôle et les sanctions sont moins sévères[165]. Cela s'explique par le fait que la CIL n'effectue bien pas ses missions de contrôle et les sanctions sont moins sévères[166].

Après avoir évoqué le contrôle à priori de la mise en œuvre des traitements, il judicieux d'analyser le contrôle à posteriori de la mise en œuvre des traitements.

[163] Art 37 de la LPDP.
[164] Certains établissements bancaires au Burkina Faso refusaient d'accomplir les formalités préalables au traitement des données personnelles. C'est quand les banques européennes ont exigé leur déclaration à la CIL comme conditions d'exécution de leurs coopérations que les banques Burkinabès ont commencé à effectuer les déclarations.
[165] La CIL devait emboiter les pas du nouveau RGPD en matière de sanction.
[166] La CIL devait emboiter les pas du nouveau RGPD en matière de sanction.

Paragraphe II : Le contrôle a posteriori de la mise en œuvre des traitements.

Il faut d'ailleurs rappeler qu'un traitement de données à caractère personnel est un ensemble d'opérations dont chacune est elle-même susceptible d'être qualifiée de traitement. Par exploitation ou mise en œuvre du traitement, nous entendons l'étape postérieure à l'accomplissement des formalités préalables et à la collecte des données. Il s'agit de la phase de traitement des données en vue de la finalité pour laquelle les données ont été collectées c'est-à-dire, en l'espèce, la conduite des traitements en vue de laquelle les données ont été collectées. Cette phase se distingue manifestement de la collecte des données.

En effet, des pouvoirs d'action sont reconnus notamment aux personnes concernées et aux autorités de contrôle pour vérifier la conformité de la mise en œuvre du traitement avec la ou les finalité(s) initialement déclarée(s), le respect des droits des personnes, la sécurité du traitement, l'utilisation des résultats obtenus.

Vérifications sur place par la Commission

La CIL dispose d'un pouvoir de contrôle sur place au sein des organismes publics ou privés et peut se faire communiquer tout renseignement ou document utile à sa mission en vue d'assurer la conformité des traitements des données à caractère personnel à la loi.

C'est pendant cette phase que la CIL vérifie la conformité des déclarations avec les finalités des traitements ainsi que les destinataires des traitements ou vérifie la compactibilité des réutilisations avec les finalités initiales. Si elle constate que les traitements ne sont pas conformes à la déclaration elle peut prononcer des sanctions administratives (mise en demeure, interruption du traitement, verrouillage de certaines données personnelles traitées, interruption temporaire ou définitive de la mise en œuvre d'un traitement etc.)[167]

Elle peut saisir la justice pour les infractions graves dont elle a connaissance[168].

Le 28 mai 2012, la CIL a procédé à des vérifications sur place dans le secteur industriel au siège de l'entreprise FTF à Ouagadougou pour effectuer une vérification sur un dispositif de vidéosurveillance, traitement de données à caractère personnel autorisé par les membres de la commission numéro 00033 du 18 mars 2011.Cette mission s'inscrivant dans le cadre de pouvoir de contrôle a posteriori reconnu à la CIL avait pour objectif spécifique de constater l'état de mise en œuvre et le fonctionnement du dispositif de vidéosurveillance au regard des

[167]CIL, Rapport public, 2012, P.5.
[168] CIL, Conseil pratique pour une meilleure protection des données personnelles, 2018, p. 5

principes et obligations que posent la loi n°010-2004/AN des recommandations de la Commission lors de sa délibération.

Au cours de la mission, l'équipe de la CIL a pu constater que le dispositif de vidéosurveillance n'étant pas opérationnel. A l'issu de la mission, l'équipe a produit un rapport dans lequel la CIL à reformuler à l'attention de l'entreprise de respecter les finalités des traitement et l'intimité de la vie privée des salariés, la reprise de l'opérationnalité du dispositif de vidéosurveillance et informer les usagers de l'entreprise de la présence des caméras de surveillance à l'aide d'affiches[169].

Dans le secteur de la téléphonie, la CIL s'est rendue le 27 septembre 2012 au siège de AIRTEL BURKINA pour une mission de vérification. Cette mission avait pour objectif d'échanger sur l'état et l'évolution des traitements de données personnelles de l'entreprise, les mesures de sécurités et de confidentialité et la localisation des bases de données[170].Cette vérification a permis au technicien de la CIL de se rendre compte que l'opérateur effectue d'important traitement des données à caractère personnel à travers ses nombreuses bases de données. A l'issu de cette mission, la CIL a, dans son rapport de mission de vérification, rappeler l'opérateur de téléphonie ses obligations en matière de traitement de données à caractère personnel

En bref, nous pouvons retenir dans cette partie nonobstant le cadre théorique de l'étude que la protection des données d'utilisateurs à caractère personnel tire sa source au niveau international et national notamment le droit européen et le droit africain et particulièrement la LPDP.Ainsi, plusieurs principes ont été élaborés et le plus innovant est l'annulation de l'autorisation et la déclaration des traitements à CIL conforment au RGPD.Dans cette analyse, nous proposons à la LPDP d'évoluer dans ce sens en raison du fait que cette procédure protège mieux les personnes concernées et élargit le pouvoir d'action de la Commission.

Après avoir étudier le cadre théorique, méthodologique et conditions d'utilisations des données à caractère personnel au Burkina Faso, il nous judicieux d'évoquer la partie suivante portant protection des données personnelles sur les programmes d'ordinateurs au Burkina Faso.

[169], CIL, Rapport public, 2012, p.12.
[170] Idem, p.15.

DEUXIEME PARTIE : PROTECTION DES DONNEES PERSONNELLES SUR LES PROGRAMMES D'ORDINATEURS AU BURKINA FASO.

Dans cette seconde partie, nous présenterons les résultats de nos enquêtes de terrain, les analyses et les interprétations qui en découlent. Le tout aboutira à la vérification de nos hypothèse chapitre (1). Puis, nous ferons des propositions en vue d'une amélioration de la situation des usagers des compagnies de transport (chapitre 2).

CHAPITRE I : PRESENTATION, INTERPRETATION DES RESULTATS ET VERIFICATIONS DES HYPOTHESES

Ce chapitre sera consacré à la présentation et à l'interprétation des résultats de nos enquêtes de terrain (Section I) d'une part et à la vérification de nos hypothèses d'autre part (Section II).

Section I : Présentation et interprétation des résultats de l'enquête

La présentation et l'interprétation des résultats se feront à l'aide de deux (2) paragraphes. Nous aurons une situation globale du recouvrement des questionnaires et des entretiens réalisés (Paragraphe I) et une présentation détaillée des questionnaires recouvrés et entretiens réalisés (Paragraphe II).

Paragraphe I : La situation du recouvrement des questionnaires et des entretiens réalisés

Nous présenterons d'abord l'état du recouvrement des questionnaires (A) puis des différents entretiens réalisés au cours de l'enquête (B)

A. La situation des questionnaires recouvrés

Les questionnaires ont été effectivement adressés aux usagers et aux dirigeants des compagnies de transport TSR et RAHIMO TRANSPORT, aux responsables administratives de la CIL et au Directeur Général de MTOPO. En effet, nous estimons que ces derniers sont mieux indiqués pour nous fournir des réponses objectives aux questions qui leur ont été posées. Ainsi pourront-ils nous renseigner sur les difficultés qui sont rencontrées par les voyageurs dans le cadre de la protection de leurs données personnelles ? Ainsi, tous les responsables administratifs de la CIL ont effectivement renseigné les questionnaires qui leur ont été effectivement adressés. Donc, tous les trois (03) responsables n'ont pas pu nous retourner nos questionnaires parce qu'ils n'avaient pas le temps. Au niveau des usagers de RAHIMO TRANSPORT, nous enregistrons 98% de taux de recouvrement soit 198 questionnaires renseignés. Après déduction, 2% des voyageurs n'ont pas pu répondre à nos questions soit deux (02) questionnaires non retournés. Enfin, pour ce qui concerne les usagers de TSR, 783 personnes ont répondu à nos questionnaires soit un taux de 97,87. Le tableau ci-dessous fait le récapitulatif de la situation.

Tableau I: situation de recouvrement des questionnaires

Population cible	Echantillon	Nombre de répondants	Taux (%)
Responsable de la CIL	03	00	00
Voyageurs du RAHIMO	200	198	98
Voyageurs du TSR	800	783	97,88
Total	**1003**	**981**	**97,8**

Source : résultats de nos enquêtes, Février -mars 2019.

Après la présentation de la situation des questionnaires recouvrés, nous allons nous intéresser à celle des entretiens réalisés.

B. La situation des entretiens réalisés

Nos guides d'entretien devaient être adressés aux Dirigeant de RAHIMO TRANSPORT, de TSR et de Directeur Général de MTOPO PAYMENT SOLUTIONS BF, nous avons un taux de réalisation de 33, 33% soit 2 entretiens réalisés au sein de RAHIMO TRANSPORT. Concernant MTOPO, seul l'entretien du Directeur Général a pu se réaliser. Le tableau ci-dessous résume la situation des entretiens

Tableau II: situation des entretiens réalisés

Personnes concernées	Entretiens prévus	Entretiens réalisés	Taux (%)
Les Dirigeants de RAHIMO	03	01	33,33
Les dirigeants du TSR	03	01	33,33
Directeur Général de MTOPO	01	01	100
Total	**07**	**03**	**42,86**

Source : Résultat de nos enquêtes février-mars.

Les deux (02) tableaux font le récapitulatif des questionnaires et guides d'entretien qui devaient être administrés à notre public cible. Ils (les tableaux) font également la situation des outils qui ont été effectivement administrés. Nous allons passer à la présentation détaillée de ces données.

Paragraphe II : Présentation détaillée des résultats de l'enquête

Dans ce paragraphe seront présentées plusieurs données issues de nos enquêtes de terrain. Il s'agit de voir si les entreprises exploitant le logiciel CONEKTO TRANSPORT protègent efficacement les données personnelles des voyageurs(A). Nous présenterons également les relations qui existent entre les différents acteurs dans le but d'assurer une meilleure protection des données collectées(B). Enfin, nous verrons si les voyageurs sont informés de leurs droits sur la protection des données à caractère personnel(C).

A. La présentation de la protection ineffective des données personnelles des utilisateurs par les intervenants du logiciel CONEKTO TRANSPORT.

A l'intention des voyageurs des compagnies de transport, un questionnaire subdivisé en plusieurs parties leur a été adressé. Sur un total de 983 voyageurs interrogés, 52,19% estiment qu'il y'a absence d'information des traitements des données personnelles, 30,92% ne connaissent pas le niveau de protection des données personnelles par les responsables des traitements. Pendant ce temps, 16,89% n'ont pas une idée sur la protection des données personnelles.

Tableau III: Protection ineffective des données personnelles des utilisateurs par les intervenants du logiciel CONEKTO TRANSPORT

Réponses	**Nombre**			
Catégories	**H**	**F**	**T**	**Taux (%)**
Non connaissance du niveau de protection des données personnelles	205	99	304	30,92
Absence d'information des finalités des traitements de leurs données personnelles	410	103	513	52,19
Pas une idée sur la protection des données personnelles	96	70	166	16 ,89
Total	**711**	**272**	**983**	**100**

Source : résultat de nos enquêtes, Février-mars 2019.

A la question de savoir si les déclarations des traitements ont été effectuées à la CIL, les dirigeants des compagnies de transport répondent : « *Non* ». Ces derniers ignorent l'existence d'une législation en matière de protection des données personnelles et une commission chargée de la protection des données personnelles au Burkina Faso.

Quant au Directeur Général de MTOPO PAYMENT SOLUTIONS BF, les compagnies de transport sont exclusivement responsables des traitements des données personnelles et de ce fait, c'est à ces dernières d'accomplir la formalité de déclaration à la CIL et de mettre en œuvre des mesures techniques et organisationnelles dans le cadre de la protection des données d'utilisateurs à caractère personnel.

Après la présentation des résultats sur la protection ineffective des données personnelles par les responsables des traitements, il faut à présent s'intéresser à la relation existante entre les intervenants dans la protection des données personnelles des voyageurs.

B. Les relations existantes entre les intervenants dans le cadre de la protection des données personnelles.

De façon concrète, cette question a été posée aux dirigeants des compagnies de transport de manière suivante : Existe-il une relation entre les différents acteurs dans le but d'assurer une meilleure protection des données collectées ? Ils doivent répondre par oui ou non et justifier.

Les dirigeants des compagnies de transport lors de l'entretien nous répondent :« Non ». Comme justification, ils disent que chacun à sa politique de gestion des données personnelles, qu'ils ont élaboré des identifiants empêchant toute personne non autorisée d'accéder aux données.

La même question a été posée au Directeur Général de MTOPO, il répond : « *il n'existe pratiquement pas une politique collective en matière de protection des données personnelles des voyageurs. Chaque entreprise a sa politique de protection. Nous déclinons notre responsabilité à l'égard des traitements effectués par les compagnies de transport, nous n'avons pas accès aux données des voyageurs sans le consentement des compagnies de transport, et par conséquent MTOPO est une entreprise de l'information, donc un hébergeur des données comme Amazon. Pour une meilleure protection des données personnelles, nous avons mis en place une politique de sécurité, la charte des risques et la matrice des risques. Nous devenons responsables des traitements en cas de réservation en ligne des billets de transport à travers l'application mobile NTERI, donc nous somme dans l'obligation de déclarer ces traitements puisque l'historique des traitements seront stockées dans notre base de données pendant plusieurs années* ».

Cette déclination de la responsabilité de MTOPO PAYMENT SOLUTIONS BF à la charge de leurs clients en matière de la déclaration des traitements des données, est contraire à toutes les règles en matière de protection des données à caractère personnel. En effet, conformément, à toutes ces législations les éditeurs d'un site internet ou d'un logiciel qui collectent les données personnelles sont dans l'obligation soit d'effectuer une simple déclaration à la CIL soit demander son autorisation en cas d'exploitation de certaines données jugées sensibles.

Après avoir évoqué les relations existant entre les différents acteurs, nous verrons comment les données personnelles sont réutilisées sans le consentement des personnes concernées.

C. La réutilisation des données personnelles des voyageurs à d'autres fins sans le consentement des voyageurs.

A l'intention des dirigeants du TSR et RAHIMO TRANSPORT à la question de savoir si les compagnies utilisent les données personnelles des voyageurs à d'autres finalités autres que celles pour lesquelles elles ont été collectées. Ceux-ci répondent par « *oui* ».

Selon le Directeur des Affaires Financières de RAHIMO TRANSPORT, les données personnelles de ses clients sont réutilisées pour déterminer les meilleurs clients, les clients les plus fidèles et utiliser à des fins de marketings et à alimenter leurs bases de données qui pourraient être utilisées à des finalités non prévues.

Selon le comptable de TSR, les traitements des données personnelles de leurs clients à pour finalités initiales la vente des tickets, réservation des tickets en ligne, gestion des bagages et colis mais elles pourront être utilisées à d'autres finalités telles que les domaines de recherches scientifiques, à des fins marketings et de publicité.

A la question de savoir s'ils ont reçu le consentement de leur client avant la réutilisation de leurs données, ceux-ci répondent : « *Non* ». Comme justification, ils disent qu'ils ne savaient pas qu'ils étaient dans l'obligation de requérir le consentement de leurs clients pour exécuter telles finalités.

Après la présentation des résultats relatifs à la réutilisation des données personnelles, nous évoquerons celle de l'absence de d'information des voyageurs de leurs droits.

D. L'absence d'information des voyeurs de leur droit à la protection des données personnelles.

A l'intention des dirigeants des compagnies de transport, avez-vous informé les voyageurs de leurs droits sur la protection des données personnelles, ceux-ci répondent par : *« non »*.

Selon le DAF du RAHIMO TRANSPORT, nous ne connaissons même pas les droits des voyageurs, comment pourrons-nous les informer sur quelque chose que nous ne connaissons pas. Quant au directeur comptable du TSR, nous ne savons pas que les données personnelles font l'objet de protection, donc nous ignorons l'existence de tels droits à l'égard des personnes concernées.

Cette même question a été soumise à quelques voyageurs du TSR et de RAHIMO TRANSPORT. Sur le total de 983 voyageurs, tous les voyageurs disent qu'ils ne sont pas informés de leurs droits sur la protection des données personnelles par les responsables de traitement de leurs données nominatives.

Tableau IV: Absence d'information des voyageurs de leurs droits sur la protection des données personnelles.

Question	**Réponse**	**Nombre de voyageurs**	**Taux (%)**
Etes- vous informés de vos droits sur la protection des données personnelles ?	Non	983	100%
TOTAL		**983**	**100%**

Source : résultat de nos enquêtes, février -mars.

La présentation et l'interprétation des résultats de l'enquête nous amènent à la section consacrée à la vérification de nos hypothèses.

Section II : La vérification des hypothèses

Dans cette section, il s'agira de procéder à la vérification de l'hypothèse principale (Paragraphe I) et des hypothèses secondaires (Paragraphe II).

Paragraphe I : Vérification de l'hypothèse principale

Dans la partie théorique de notre étude, nous avons estimé comme hypothèse principale que les données à caractère personnel des personnes concernées par le traitement sont souvent détournées à d'autres finalités que celle pour laquelle elles ont été collectées. Il s'agit, dans cette partie, de voir si cette hypothèse se vérifie dans la pratique. Selon les dirigeants des compagnies de transport, les données personnelles des voyageurs sont utilisées à des finalités autres que la vente des tickets consentie par les voyageurs sans leurs consentements. Selon l'article 14 de la LPDP, les données doivent être collectées pour des finalités déterminées, explicites et légitimes. En conséquence, les données ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été collectées alors que les responsables de transport le font sans le consentement des voyageurs ni les informer des différentes finalités ultérieures au traitement. Ces comportements sont une violation systématique des droits des personnes concernées en raison du fait que c'est la manière dont les données sont traitées qui peut mettre à mal la vie privée des voyageurs.

En outre, 304 voyageurs, donc 30,92% des voyageurs ne connaissent pas le niveau de protection de leurs données personnelles par les responsables de traitement, ce qui est en contradiction avec l'article 17 de la LPDP. En effet, l'alinéa 1 de cet article donne la possibilité aux personnes concernées « *de connaître les données conservées qui les concernent* ». Ce droit doit être effectif et doit pouvoir être exercé sans délai ou frais excessifs. Cependant, l'exercice de ce droit par les personnes concernées pour s'enquérir auprès des responsables des traitements le niveau de traitement des données personnelles, connaitre la compatibilité des traitements avec les finalités initiales des traitements et des mesures organisationnelles et techniques mises en place par les responsables des traitements dans le cadre d'une meilleure protection de leurs données personnelles.

Toutes les deux compagnies de transport n'ont pas effectué les formalités préalables (déclarations et autorisations) au traitement des données ce qui est en déphasage avec la loi du 24 avril 2004.En effet, conformément à l'article 19 et suivant de la LPDP tout personne physique ou morale décidant de la création des données personnelles à l'obligation de faire la

déclaration des traitements à la CIL avant la mise en œuvre des traitements. C'est pendant l'accomplissement des formalités administratives que les responsables des traitements déterminent explicitement les finalités des traitements, les destinataires des traitements et les sous-traitants, les possibilités de transfert à l'étranger des données personnelles et la limitation de la durée de conservation des données.

Par conséquent, notre hypothèse principale se vérifie en pratique car 100% des responsables des traitements collectent des données à d'autres fins autres que celles consenties par les voyageurs.

L'hypothèse principale étant vérifiée, nous allons nous appesantir sur la vérification des hypothèses secondaires.

Paragraphe II : Vérification des hypothèses secondaires

Les hypothèses secondaires au nombre de trois (3) seront vérifiées dans ce paragraphe. Il s'agit d'une part de la protection ineffective des données d'utilisateurs à caractère personnel par les responsables de traitement(A), d'autre part, il n'existe aucune relation entre les différents intervenants dans la protection des données personnelles(B) et enfin les personnes concernées ne sont pas informées de leur droit sur la protection de leurs données personnelles(C).

A. La protection ineffective des données d'utilisateurs à caractère personnel

A ce niveau, nous avons relevé que les données personnelles des voyageurs ne sont pas protégées de façon efficace par les responsables des traitements. Ainsi avons-nous souligné que les personnes concernées ne connaissent pas le niveau de protection de leurs données personnelles, qu'ils n'ont pas une idée sur la protection des données personnelles et que les responsables des traitements n'exécutent pas leur obligation d'information. Pour vérifier ces hypothèses, nous avons adressé des questionnaires aux voyageurs des compagnies de transport du TSR et RAHIMO TRANSPORT. Les données de l'enquête sont consignées dans le tableau ci-dessous.

Tableau V: L'ineffectivité de la protection des données personnelles des voyageurs par les responsables de traitement.

Réponses	**Nombre**			
Catégories	**H**	**F**	**T**	**Taux (%)**
Aucune idée sur le niveau de protection des données personnelles	205	99	304	30,92
Absence d'information	410	103	513	52,19
Pas une idée sur la protection des données personnelles	96	70	166	16 ,89
La protection est efficace	00	00	00	00
Total	711	272	983	100

Source : résultats de nos enquêtes février-mars.

En résumé, les chiffres sont les suivants :

- 30,92% des voyageurs disent qu'ils ne connaissent pas le niveau de protection de leurs données personnelles ;
- 52,19 % des voyageurs trouvent que les responsables de traitement n'exécutent pas leur obligation d'information ;
- 16,89% des voyageurs n'ont pas une idée sur la protection des données personnelles et
- 00% des voyageurs sur la protection efficace.

En définitive, cette hypothèse est vérifiée car tous les voyageurs estiment que leurs droits ne sont pas protégés efficacement. Cela se confirme par le fait que les compagnies de transport n'informent pas les voyageurs des destinataires de leurs données, la durée de conservation et les autres finalités des traitements de leurs données personnelles qui affectent une protection efficace des données personnelles. A ce sujet, un voyageur suggère :« *il faut que la Commission de l'Informatique et des Libertés sanctionne sévèrement les responsables des traitements qui outrepassent les textes juridiques relatifs à la protection des données personnelles et sensibiliser la population sur leurs droits sur la protection de leurs données personnelles* ». Si le droit d'aller et de venir, de vivre, de disposer de son corps sont des droits connus de la plupart des citoyens, la loi burkinabé portant protection des données à caractère personnel l'est moins au regard du fait qu'elle est récente pour avoir été adoptée précisément le 20 Avril 2004. Le caractère récent de l'adoption de cette loi fait qu'elle est peu connue.

Cette méconnaissance ne se limite pas uniquement aux profanes, elle s'étend même aux étudiants en faculté de droit privé ou aux juristes en général. Cette méconnaissance de la loi est une entrave à son application. Il faut noter, par ailleurs, l'aspect technique des dispositions de cette loi. Si même les spécialistes en droit des nouvelles technologies ont parfois du mal à s'accommoder avec les termes employés par le législateur, nous comprenons bien que ce serait plus difficile pour les profanes de pouvoir la comprendre. Pour l'application matérielle de la loi, il faudrait la constitution d'un fichier. Toutefois, malgré les explications données par l'article premier de la loi burkinabè portant protection des données à caractère personnel, la compréhension du terme fichier n'est pas claire dans les esprits.

Selon les statistiques de l'UNESCO, le taux d'alphabétisation au Burkina Faso est de 59%. Aux dires de la Ministre de l'éducation nationale et de l'enseignement technique, ce taux jugé faible, constitue un frein au développement humain durable. Ce problème d'alphabétisation que connaît la population est en partie la cause de la méconnaissance de la loi.

L'analphabète qui ne sait ni écrire et ni lire, peut-il s'intéresser à des dispositions légales qui se rapportent à la protection de ses données personnelles, lorsque toutes ces expressions sont pour lui un langage inaccessible. Il saisit à peine l'intérêt de tous ces textes qu'il ignore d'ailleurs. L'analphabétisme est donc un frein à la connaissance de la loi relative aux données à caractère personnel. C'est conscient de ce fait que lors de la journée d'alphabétisation, la Ministre de l'éducation s'est fixée comme objectif de faire baisser considérablement ce taux à 35%. Elle a donc, pour atteindre cet objectif, invité les populations analphabètes à se familiariser avec la lecture, l'écriture et le calcul, afin de s'épanouir, de s'ouvrir au développement, aux innovations. Mais comment une personne qui ne sait ni lire ni écrire peut-elle se familiariser avec la lecture si elle n'a pas de formation en la matière.

La vérification de cette hypothèse nous conduit ainsi à la vérification de la deuxième hypothèse qui a trait à la relation existante entre les différents intervenants sur le logiciel dans la protection des données personnelles des voyageurs.

B-Absence de relation entre les différents intervenants dans la protection des données personnelles.

La vérification de cette hypothèse a été possible grâce au guide d'entretien qui a été adressé au Directeur Général de MTOPO, aux dirigeants de TSR et RAHIMO TRANSPORT. Il s'agit pour nous de connaitre si les responsables des traitements protègent collectivement les données personnelles des voyageurs.

Pour ce faire, la question suivante leur a été posée : « *Avez-vous prévu une politique collective de protection des données personnelles avec vos partenaires ?* ».

Tableau VI: Absence de relation entre les différents intervenants du logiciel dans le cadre de la protection des données personnelles des voyageurs.

Réponses	**Nombre**			
Catégories	**H**	**F**	**T**	**Taux**
Oui	00	00	00	00
Non	03	00	03	100
Total	3	00	3	100

Source : résultat de nos enquêtes Février-Mars 2019

Cette hypothèse est à 100% vérifiée car les personnes avec qui nous sous sommes entretenues affirment qu'il n'existe pas une politique de protection des données personnelles avec leurs partenaires. Les différents intervenants n'ont pas utilisé la possibilité qui leur est offerte par la commission à travers laquelle si plusieurs entreprises exploitent en commun un logiciel, elles ont la faculté de choisir un responsable principal pour accomplir les formalités de déclaration à la CIL et de mettre en place des mesures organisationnelles et techniques dans le cadre d'une meilleure protection des données personnelles des utilisateurs. La protection collective des données personnelles par les intervenants permet de déléguer la partie la plus diligente et professionnelle pour veiller à une meilleure protection des données sur le logiciel.

La vérification de cette hypothèse nous conduit ainsi à la vérification de la troisième hypothèse qui a trait à l'absence d'information des voyageurs de leurs droits des données personnelles.

C. Les personnes concernées ne sont pas informées de leur droit sur la protection des données personnelles.

La vérification de cette hypothèse a été fructueuse grâce à nos questionnaires et guide d'entretien adressés respectivement aux voyageurs et aux dirigeants des compagnies de transport. Pour ce faire, la question suivante a été posée aux voyageurs : « *Etes-vous informés de vos droits sur la protection de vos données personnelles ?* ».

Les données de l'enquête sont consignées dans les tableaux ci-dessous.

Tableau VII: Absence d'information des voyageurs de leurs droits.

Réponses	**Nombre**			
Catégories	**H**	**F**	**T**	**Taux**
Oui	00	00	00	00
Non	03	00	03	100
Total	**3**	**00**	**3**	**100**

Source : résultat de nos enquêtes février-mars 2019

Pour les responsables de traitement cette question leur a été posée : *« Avez-vous informé les voyageurs de leur droit sur la protection des données personnelles ?* »

Tableau VIII: Absence d'information des voyageurs de leurs droit**s**

Réponses	**Nombre**			
Catégories	**H**	**F**	**T**	**Taux**
Oui	00	00	00	00
Non	711	272	983	100
Total	711	272	983	100

Source : résultat de nos enquêtes février-mars 2019

Cette hypothèse est à 100% vérifiée aussi car les personnes avec qui nous nous sommes entretenues et auxquelles nous avons soumis nos questionnaires affirment que les responsables des traitements n'informent pas les personnes concernées de leurs droits sur la protection de leurs données à caractère personnel, l'absence d'information des voyageurs de leurs droits dans le contrat de transport des conditions d'exercice de leurs droits .Cela montre aussi une inaction de la Commission dans l'information et la sensibilisation des citoyens de leurs droits sur la protection de leurs données personnelles et de la promotion de cette loi nouvelle.

Pour un journaliste de la chaîne de télévision nationale, rares sont ceux qui prétendront ne pas connaître la caisse nationale de la Sécurité Sociale (CNSS) à travers ses campagnes de sensibilisation sur cette chaîne de télévision. Par ces campagnes, même les plus jeunes ont une connaissance plus ou moins approfondie des missions de la CNSS et de son domaine. Il en est de même pour les campagnes de sensibilisation relatives au paiement d'impôts. Cette campagne est appuyée par des consultations en direct. Si la CNSS par ce canal est bien connue, la CIL par

contre est méconnue de la population car nombreux sont ceux qui ignorent son existence. Pour les mieux informés, CIL est connue en tant Commission de l'Informatique et des Libertés. Cette méconnaissance de la CIL en tant qu'organe chargé de la protection des données à caractère personnel lui est imputable. La CIL sur sa page officielle Facebook ou sur son site internet s'affiche plus en tant qu'autorité de protection des données personnelles. Ce défaut d'information sur la CIL et ses missions entravent la protection efficace des données personnelles puisque les personnes concernées par le traitement ne sont pas informées sur la possibilité d'un quelconque recours et de l'organe qui prendrait en charge leur requête.

Les données qui viennent d'être présentées sont issues de nos enquêtes de terrain courant février-mars 2019. Et à y observer, on se rend compte que les données personnelles des voyageurs ne sont pas protégées par les compagnies de transport. C'est pourquoi, afin de résoudre ces difficultés des propositions sont faites dans le chapitre qui suit.

CHAPITRE II : DES PROPOSITIONS DES SOLUTIONS POUR AMELIORATION DES DROITS DES VOYAGEURS ET D'AUTRES PERSONNES CONCERNEES

Au regard des résultats de notre enquête, la protection des données personnelles des voyageurs par les responsables des traitements est ineffective. Il est donc nécessaire de mettre en place des stratégies nécessaires pour une meilleure protection des données personnelles des voyageurs et des personnes concernées en général. Pour une meilleure protection des données personnelles des personnes concernées, nous proposons, d'une part, des reformes législatives et des mesures de sensibilisation (section I) et d'autre part les mesures à prendre par les utilisateurs et par les responsables des traitements pour sécuriser les données à caractère personnel (section II)

Section I : Les reformes législatives et les mesures de sensibilisation.

Les compagnies de transport en particulier et en général beaucoup d'entreprises responsables de traitement ne protègent pas efficacement les données personnelles de leurs clients ,ce qui constitue une violation de leurs obligations et les droits des personnes concernées .Cela se justifie par la complexité et le manque de la promotion de la LDPD .Pour remédier à cela, nous proposons, d'une part, des reformes législatives (Paragraphe I) et d'autre part, les mesures de sensibilisations(paragraphe II).

Paragraphe I : Les reformes législatives

A-L 'extension du champ d'application de la LPDP

Selon l'article 8 LPDP «la présente loi s'applique aux traitements automatisés ou non de données à caractère personnel contenues ou appelées à figurer dans les fichiers ». Le législateur restreint le champ d'application matériel de la loi[171]. Cela voudrait dire par exemple que la loi n'a vocation à s'appliquer aux traitements automatisés que s'il y a constitution d'un fichier. Pourtant, cela est en déphasage total avec l'ensemble des législations de protection des données qui se sont toujours appliquées aux traitements automatisés de données à caractère personnel en principe. Les traitements non automatisés n'étant concernés que s'il y a constitution de fichiers. Quant au champ d'application territorial, elle s'applique au traitement effectué au Burkina Faso et hors du Burkina Faso. Facebook, WhatsApp, Integram, télégram et

[171] Article 8 de la LPDP.

bientôt Town square, les sites de socialisation attirent de plus en plus de membres, de toutes tranches d'âge et de toutes nationalités. Néanmoins, les utilisateurs n'ont pas toujours conscience des risques encourus en éparpillant des informations personnelles sur ces sites. En outre, ces sites de socialisation sont situés le plus souvent hors du continent africain[172]. Le législateur doit étendre le champ d'application à tous les traitements qu'ils soient automatisés ou pas sans faire référence à l'établissement d'un fichier, c'est-à-dire étendre aux traitements automatisés de données personnelles effectués en l'absence de constitution de fichier. En outre, le caractère d'application hors national de la loi suscite des interrogations parce que difficile à mettre en œuvre par les personnes concernées. De ce fait, le législateur doit prévoir des techniques d'applicabilité de cette loi hors du Burkina pour une protection effective des données personnelles des personnes vivantes au Burkina Faso, membres des réseaux sociaux.

Certaines contradictions peuvent aussi être relevées concernant par exemple la disposition de l'article 11 qui prévoit que la loi ne s'applique pas aux traitements de données ayant pour fin le suivi thérapeutique ou médical des patients alors que par l'application de nombres de dispositions de la loi (articles 17, 20, 21, 23), ces traitements se trouvent cernés par la loi[173]. Enfin, certaines formulations s'avèrent maladroites entraînant une incertitude sur le contenu de la loi. A la lecture de l'article 14, par exemple, on peut se poser la question de savoir si la réutilisation des données est-elle admise ou non. En effet, si l'alinéa premier prévoit que les données ne peuvent être utilisées qu'en vue des finalités pour lesquelles elles ont été collectées, ce qui exclut a priori toute réutilisation. L'alinéa 2 semble admettre cette réutilisation en prévoyant la proportionnalité des données «au regard des finalités pour lesquelles elles sont traitées ultérieurement ». Le législateur doit pouvoir départager ces contradictions des dispositions qui rendent difficiles la compréhension des dispositions de ces articles par les profanes.

Le législateur burkinabé doit également tirer une leçon sur quelques principes du nouveau règlement général sur la protection des données personnelles de l'Union Européenne [174]notamment le principe de la tenue d'un registre de traitement des données(Article 30), coopération avec l'autorité de contrôle(Article 31),notification à l'autorité de contrôle de la violation de données à caractère personnel ,communication à la personne concernée de la violation, l'analyse d'impact relatif à la protection des données personnelles(Article 55) et

[172] Les GAFAM sont des sociétés de nationalités américaines mais dispose au Burkina Faso des moyens qui collectent des données personnelles des Burkinabès. Le législateur burkinabé doit étendre le champ d'application de la loi hors du Burkina tout comme le nouveau RGPD afin de responsabiliser les entreprises siégeant à l'étranger mais disposant au BF des moyens de collecte des données personnelles.

[173] Des reformulations doivent être faites en vue d'expliciter les dispositions de ces articles.

[174] Articles 30 ,31 et 55 du RGPD.

consultation préalable, désignation d'un délégué à la protection des données personnelles et l'élaboration d'un code de conduite. La tenue du registre est indéniablement importante que l'accomplissement des formalités préalables à la CIL en raison du fait qu'elle permettra à ce dernier d'effectuer des contrôles à tout moment sans attendre les déclarations et de réduire ses insuffisances.

La LPDP n'a pas prévu des dispositions spécifiques régissant les réseaux sociaux alors qu'ils sont aujourd'hui des véritables canaux de vulgarisations des informations personnelles qui mettent à mal la vie privée des membres par les géants du net. Il faut une législation en ce sens à l'exemple de la Cote D'ivoire qui a été très vigilent dans la rédaction quant à l'institution des règles spécifiques responsabilisant les responsables des réseaux sociaux[175]. Il faut étendre également les conditions d'utilisation des applications mobiles et les obligations des responsables des traitements.

Nous proposons également au législateur burkinabé d'insérer une partie des dispositions de la LPDP dans le code du travail, notamment la protection de la vie privée des travailleurs dans les lieux du travail[176]. L'intérêt de cette insertion est qu'elle permettrait non seulement aux travailleurs de connaitre leurs droits, mais aussi de pouvoir les mettre en œuvre comme les autres dispositions du code de travail supposées les plus maitrisées par les citoyens. Après avoir apporté des propositions sur l'extension du champ d'application de la loi, nous verrons comment étendre le pouvoir de contrôle et de sanction de la commission.

B.L 'extension du pouvoir de contrôle et de sanction de la commission

Nous pensons que l'extension du pouvoir d'action et de sanction de la CIL à l'égard des violataires des règles de protection des données personnelles s'avère nécessaire à une meilleure protection des données personnelles. En effet, le pouvoir conféré à la CIL en matière de contrôle est très restreint et ne permet pas à celle-ci de veiller à une meilleure protection des données personnelles des utilisateurs en raison du fait que le système est déclaratif. Le contrôle a posteriori de la mise en œuvre des traitements est le seul moyen permettent à la commission d'effectuer les vérifications sur place. Le contrôle sur place avant la déclaration est plus pertinent que celui postérieur à la déclaration.

[175] Article 41 al 3 de la loi ivoirienne portant protection des données à caractère personnel.
[176] La protection des données personnelles des travailleurs dans les lieux de travail est régie spécifiquement par le code de travail. L'obligation d'information préalable résulte de l'article L 121-8 du code du travail francais.Par ailleurs, l'article L 432-2-1 prescrit que le comité d'entreprise doit être "informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

En effet, la commission pourrait mettre en place une commission d'enquête chargée de vérifier la conformité des traitements des données personnelles avec la LPDP aux seins des entreprises et de formuler des recommandations demandant à ces dernières d'effectuer des déclarations dans des brefs délais. En cas d'inobservations à ces recommandations, la CIL pourrait leur infliger des sanctions sévères conformément au texte en vigueur.

Les sanctions prévues par la LPDP ne sont pas appliquées. Ces dispositions prises dans le cadre de la protection des données à caractère personnel sont à saluer. Cependant, elles ont une portée restreinte. En plus, les différentes sanctions édictées sont moins sévères ce qui pourrait être disproportionné à la violation constatée. Le législateur burkinabé, quant à lui, a consacré huit(8) articles à la répression des violations des données personnelles telles que : « *le fait de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi ; le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité desdites informations, notamment empêcher qu'elles ne soit déformées, endommagées, ou communiquées à des tiers non autorisés ; le fait de communiquer à des tiers non autorisés ou d'accéder sans autorisation ou de façon illicite aux données à caractère personnel ; le détournement de finalité d'une collecte ou d'un traitement de données à caractère personnel ; le fait de collecter des données par un moyen frauduleux, déloyal, ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré son opposition, lorsque cette opposition est fondée sur des raisons légitimes ; le fait de mettre ou de conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales, ethniques ou les opinions politiques, philosophiques, ou religieuses ou les appartenances syndicales ou les mœurs des personnes ; le fait, sans l'accord de la Commission de l'informatique et des libertés, de conserver des informations sous une forme nominative au-delà de la durée prévue à la demande de l'avis ou à la déclaration préalable à la mise en œuvre du traitement informatisé ; le fait, pour toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à l'honneur et à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ; le fait d'entraver l'action de la commission ».* De ce fait, la Commission devrait revoir ce cas, en formulant des mesures et recommandations à l'égard du gouvernement et à l'Assemblée Nationale portant modification de ces dispositions. Comme

proposition de projet d'adaptation de la loi, nous proposons à la CIL de tirer exemple des sanctions prévues, notamment par le RGPD. Le RGPD prévoit des sanctions administratives aux responsables de traitement fautifs allant jusqu'à 20 000 000 d'euros, et s'il s'agit d'une entreprise, allant jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précèdent. Cette disposition si elle est adoptée par le Burkina Faso aura pour conséquence une sensibilisation des entreprises et autres responsables de traitement de données personnelles relative à la manière dont ils gèrent leur politique d'exploitation des données personnelles. Cette lourde sanction si elle est appliquée de plein droit permettrait de réduire les infractions à la LPDP.

En plus des propositions d'un projet de modification de la LPDP, la sensibilisation des différents acteurs à la protection des données personnelles et les personnes concernées est nécessaire.

Paragraphe II : La sensibilisation des différents acteurs à la protection des données personnelles et les personnes concernées.

Pour améliorer la protection des droits des personnes concernées par le traitement, il serait impérieux pour la Commission de procéder à une meilleure sensibilisation des dirigeants des compagnies de transport (A) et la sensibilisation des personnes concernées de leurs droits sur la protection des données personnelles(B).

A. La sensibilisation des responsables de traitement sur leurs devoirs.

La Commission de l'Informatique et Libertés devrait organiser des séminaires de sensibilisation au profit des dirigeants des compagnies de transport et MTOPO sur les mesures à prendre pour une meilleure protection des données à caractère personnel des personnes concernées dont ils accèdent, conformément à la LPDP. De ce fait, ce séminaire informerait les responsables de traitement de leurs obligations sur la protection des informations personnelles des voyageurs et les droits des personnes concernées par le traitement en les recommandant, a priori, d'accomplir les formalités de déclaration des traitements à la CIL, ce qui permettrait à cette dernière de vérifier ultérieurement la conformité des déclarations des traitements à travers son pouvoir de contrôle au sein des responsables. En outre, il permettrait aux responsables de connaitre les droits des personnes concernées et d'informer ces derniers en cas de traitement. La déclaration permettrait à la Commission de limiter les traitements des données suivant une

autre finalité ultérieurement qui serait incompatible avec la finalité initiale et la durée de conservation des données personnelles.

Par ailleurs, pour atteindre tous les acteurs et les responsables de traitement des entreprises privées et semi privées, la CIL pourrait organiser des séminaires au moins deux (02) fois par an au sein de la Chambre de Commerce et de l'Industrie invitant tous les responsables à une participation obligatoire. Le défaut de cette participation serait passible de sanction sévère sauf en cas survenance d'un cas de force majeur. Cette participation obligatoire de ces dirigeants aux séminaires permettrait non seulement de faire la promotion de la LPDP et d'informer ces derniers de leurs obligations en matière de protection des données personnels sur l'internet et sur les lieux de travail.

La sensibilisation des responsables de traitement sur leurs devoirs nous amène également à sensibiliser les personnes concernées sur leurs droits et devoirs en matière de protection des données personnelles.

B. La sensibilisation des personnes concernées

Dans le cadre d'une meilleure sensibilisation des personnes concernées, la CIL doit les sensibiliser sur leurs droits et devoirs (1) d'une part et d'autre part sur les risques liés à la mise à disposition de leurs données personnelles (2).

1. Les sensibilisations sur leurs droit et devoirs

A partir de 2004, le Burkina Faso a adopté de nombreux textes normatifs dans le domaine des Nouvelles Technologies de l'Information et de la Communication (NTIC). Il s'agit, notamment, de la loi relative à la protection des données à caractère personnel et de la loi relative aux transactions électroniques. L'appréhension de ces dispositions est difficile même pour les juristes encore moins pour les profanes[177]. La CIL, doit, donc, porter à la connaissance des citoyens, leurs droits relativement à la protection des données personnelles. Ainsi, ils doivent être éclairés sur les actes qui pourraient constituer une violation de leurs données personnelles. La CIL, doit, par ailleurs, faire connaître aux citoyens les instances vers lesquelles ils peuvent s'orienter pour obtenir gain de cause. La protection des données personnelles n'est

[177] I.COU LIBALY, La difficile appréhension du droit émergent des NTIC en Côte d'Ivoire, disponible sur « http://www.village-justice.com/articles/difficile-apprehension-droit,18339.html#SALiq0wsldgElWG7.99 »,(Consulté le 09 décembre 2018 à 15h).

pas uniquement valable pour ses propres données personnelles, mais aussi pour ceux des autres personnes. Ainsi, la sensibilisation doit porter, en outre, sur les devoirs des utilisateurs notamment l'abstention de divulguer les données des autres membres sans leur consentement. En d'autres termes, ils doivent être exhortés au respect des données personnelles des autres membres. Il faut noter que pour terminer, ces campagnes doivent être menées de telle sorte à atteindre les cibles visées.

Pour informer les personnes concernées de leurs droits sur la protection de leurs données personnelles, outre les publications sur le site de la CIL et les radios, la commission pourrait faire des publications des droits des personnes concernées sur les réseaux sociaux les plus visités par les citoyens, tels que YouTube, WhatsApp, instegram, télégramme et Facebook. Pour se faire, elle peut créer des comptes sur YouTube, WhatsApp et Facebook, puis publier quotidiennement des vidéos, des images sous forme de dessins animés dans toutes les langues parlées au Burkina Faso, qui diffuseraient les facteurs de risques de la violation de la vie privée des personnes physiques par les TIC et informeraient les personnes concernées de leurs droits. La publication des droits des personnes concernées sur ces réseaux permettrait aux utilisateurs de les connaitre et de les mettre en œuvre. L'avantage de ces publications est non négligeable en raison du fait qu'elles permettraient aux utilisateurs de s'informer et de diffuser ces publications aux autres utilisateurs des réseaux sociaux. L'accès à ces informations permettrait aux utilisateurs, en général, d'avoir une idée sur la protection de leurs informations personnelles et de prendre des meilleures précautions pour maitriser les facteurs de risques susceptibles de porter atteinte à leur intégrité morale et, en général, la violation de leur vie privée.

Cette publication pourrait porter également sur les enjeux économiques et politiques des GAFAM qui sont des entreprises de technologies les plus puissantes du monde en matière de traitement des données personnelles. En effet, les données personnelles des utilisateurs sont l'objet de vente par ces entreprises à d'autres entreprises. En outre, l'accès des données personnelles permettrait aux responsables de contrôler la masse de population. Après le téléchargement de ces applications, ces entreprises mettent à la disposition des utilisateurs des conditions d'utilisation et une politique de confidentialité dont ces derniers devront accepter avant l'ouverture de leur compte. Les utilisateurs devront prendre le soin de lire ces conditions avant d'apporter leur engagement afin de savoir si lesdites conditions ont prévu une clause de protection de leurs informations personnelles. Après avoir proposé une sensibilisation des personnes concernées sur leurs droits et devoirs, la sensibilisation de ces dernières sur les risques liés à la mise à disposition de leurs données personnelles s'avère nécessaire.

2-La sensibilisation des personnes sur les risques liés à la mise à disposition de leurs données personnelles

« *Pour vivre heureux, vivons cachés* » ! Voilà un adage qui paraît bien loin des préoccupations des promoteurs de réseaux sociaux et d'une grande partie de leurs utilisateurs.

On pourrait même se demander si, pour vivre « *connectés* », il ne faut pas vivre « exhibés » ... Voyant la toile comme un univers de liberté sans contrainte, la plupart des grands vecteurs de communication actuels fondent leurs pratiques sur le postulat que tout doit être rendu public. On peut sans doute y voir l'influence du droit américain (les serveurs des réseaux sociaux les plus représentatifs se trouvent aux États-Unis) ; les États-Unis ayant toujours été plus soucieux d'éviter les restrictions sur le commerce électronique que d'assurer une protection effective des données personnelles sur Internet. Toutefois, cela correspond aussi et surtout à l'esprit de la « génération du Net » qui fait émerger une nouvelle forme de sociabilité fondée sur les échanges libres et la conversation en continue[178].

Cette nouvelle forme de sociabilité sied aux utilisateurs. La plupart des photos prises sont destinées à être postées[179]. Les mentions « *j'aime* » et « *commentaires* » laissées par les amis ou connaissances apportent une certaine satisfaction et rendent les internautes dépendants de cette pratique. Il faut signifier que chaque jour le réseau social *Facebook* abrite au total 240 milliards d'images, soit près de 30 fois plus que *Flickr* et 70 fois plus que *Instagram*. 350 millions de nouvelles photos sont téléchargées chaque jour sur la plateforme. *Snapchat*, le service mobile permettant de partager des photos pendant une durée limite, enregistre, lui, 150 millions de nouvelles images téléchargées tous les jours[180] !

Il faut dire que les internautes ignorent que la diffusion publique d'informations sur un réseau social est bien souvent irréversible. La mémoire informatique est telle qu'il est désormais possible de conserver, sans limite de temps, toutes les informations diffusées en ligne.

La « *génération du Net* » est trop jeune pour avoir l'expérience de la mémoire du temps. Elle n'a pas conscience que la réalité finit toujours par la rattraper lorsque ressurgissent bien plus tard des images ou des informations dérangeantes, glanées sur le Net par des curieux ou de futurs employeurs. Les informations laissées par les internautes peuvent être piratées ou

---

[178] M. DAGNAUD, *Les jeunes et les réseaux sociaux : de la dérision à la subversion, disponible sur* « https://lectures.revues.org/11569 », (Consulté le 22/04/2019 à 16 h).

[179] C.Dani, L. GARINO, *Quels droit pour les réseaux sociaux ?, disponible sur «* http://laloidesparties.fr/droit-reseaux-sociaux *».*

[180] Ligue des droits de l'Homme, *Protection des données personnelles :* Analyse comparée des législations et des pratiques dans neuf pays européens dans le contexte du cadre juridique européen, disponible sur « http://www.ldh-france.org/IMG/pdf/SynthesfrancaisFINALcorr-BD.pdf », (Consulté le 9 décembre 2018).

tombées entre les mains de criminels qui s'en serviraient pour les tracer et attenter à leur vie. Cette pratique devrait donc être abandonnée. Dans le pire des cas, ils devraient filtrer les informations qu'ils publient.

En République Tchèque, des campagnes s'adressent essentiellement aux enfants[181]. Une campagne de sensibilisation devrait être organisée par la CIL, pour exhorter la jeunesse sur le partage massif de leurs informations personnelles sur les réseaux sociaux. La CIL, en vertu de sa mission de protection des données personnelles, devrait sensibiliser ces jeunes internautes sur les dangers que cette pratique présente pour leurs données personnelles. Après avoir évoqué les reformes législatives et les mesures de sensibilisations à effectuer, nous analyserons les mesures à prendre par les utilisateurs de téléphones mobiles pour sécuriser leurs données.

Section II : Les mesures à prendre par les utilisateurs de téléphone mobile et par les responsables des traitements pour sécuriser les données à caractère personnel.

Pour parvenir au respect scrupuleux de ses obligations de sécurisation des données à caractère personnel collectées, le responsable du traitement doit prendre certaines mesures. Le traitement des données personnelles par les logiciels étant un traitement automatisé, des mesures adaptées doivent être prises pour garantir la sécurité des données personnelles collectées.

La mise en place d'une sécurité physique et réseau et celle d'une sécurité logicielle s'avère nécessaire. La sécurité réseau permettrait, de garantir la sécurité des personnes concernées, quant à la sécurité physique, elle permettrait de restreindre l'accès aux données. Pour ce qui est de la sécurité logicielle, elle servirait à prévenir d'éventuelles failles du système du réseau.

Dans cette section, il sera question d'étudier, dans un premier temps, les mesures imputables aux compagnies de transport et MTOPO PAYMENT SOLUTIONS BF (Paragraphe I) et dans un second temps, les mesures à prendre par les utilisateurs de téléphones mobiles et de smartphones pour sécuriser leurs données à caractère personnel (Paragraphe II)

[181] Idem

Paragraphe I : Les mesures imputables aux compagnies de transport et MTOPO

Les responsables de traitements doivent prendre mesures efficaces afin de protéger des données personnes des personnes concernées par le traitement. De ce fait, nous proposerions à MTOPO et aux compagnies de transport de mettre en place, d'une part, la sécurité physique et réseau(A) et d'autre part, **l**a nécessité de prévoir une sécurité logicielle(B).

A. La mise en place de la sécurité physique et réseau

Le responsable du traitement, conformément à la loi relative à la protection des données personnelles, est tenu de garantir aux données collectées un niveau de sécurité suffisant. Il doit, par conséquent, mettre tous les moyens en œuvre pour parvenir à cette fin.

La restriction de l'accès physique aux serveurs et aux locaux des serveurs (1) et la sécurisation de l'accès au compte pour les internautes (2) sont des solutions envisageables.

1. La restriction de l'accès physique aux serveurs et aux locaux des serveurs

Il faut dire qu'il s'agira pour le responsable du traitement de veiller à ce que les données ne soient pas manipulées par un grand nombre de personnes. Dans le souci d'assurer aux données personnelles une certaine sécurité, l'accès aux serveurs et aux locaux des serveurs doit être restreint.

L'article 42 alinéa premier de la loi ivoirienne relative à la protection des données personnelles dispose que le responsable du traitement est tenu : « *d'empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données* ... ». Cette restriction s'étend jusqu'aux systèmes de traitement de données. L'alinéa 2 de l'article susmentionné dispose : « *Le responsable du traitement est tenu : d'empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données* ».

Aux termes de cet article, il ressort que l'utilisation des systèmes de traitements n'est pas permise aux personnes non autorisées. Ces dispositions ont pour but de garantir la sécurité des données puisque le but visé, est d'éviter toute divulgation ou modification ou tout autre incident dont les données pourraient faire l'objet. L'objectif du législateur est d'éviter qu'un grand nombre de personnes ait accès aux données collectées. Les données étant d'une importance capitale, et de nos jours des biens à valeur économique, c'est à juste titre que leur accès doit être

limité pour minimiser les risques d'insécurité. Le législateur burkinabè doit tirer une leçon de cet article.

Après avoir montré les restrictions de l'accès physique aux serveurs et aux locaux des serveurs, nous verrons comment sécuriser l'accès au compte des membres.

2. La sécurisation de l'accès aux « comptes » des membres.

La sécurité des données collectées est une obligation qui est à la charge du responsable du traitement. Cette obligation de sécuriser les données collectées transparaît à l'article alinéa 3 qui dispose :

« *Le responsable du traitement est tenu d'empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacements non autorisés de données enregistrées ...* ».

La sécurité des données collectées est un souci pour le législateur burkinabé puisque lors de la déclaration d'un traitement ou une demande d'autorisation, le responsable du traitement doit y mentionner les dispositions prises pour assurer la sécurité des traitements, la protection et la confidentialité des données traitées.

A la lecture des articles sus-évoqués, il ressort que l'obligation de sécurisation des données collectées est primordiale. Cette sécurité pour les logiciels, passe par l'adoption de mesures de sécurité efficaces. Ces mesures sécuritaires consistent à mettre en place des mots de passe à même de garantir la protection des données contenues sur le « compte » des utilisateurs. En d'autres termes, ces mots de passe doivent pouvoir protéger efficacement l'accès aux comptes des utilisateurs. Compte tenu des progrès des outils de contournement des mots de passe (Tables Arc en ciel) et de la rapidité des ordinateurs, un bon mot de passe doit :

- Avoir une longueur minimale de 14 caractères ;
- Être une combinaison de majuscules / minuscules / chiffres et signes spéciaux ou accentués ;
- Il ne doit pas être identique ou proche ou dérivé de votre identifiant (login - User Name) ;
- Il ne doit pas être constitué de votre nom et/ou de votre prénom, ni de leurs initiales, ni d'aucun nom (patronyme) et/ou prénom existants dans des dictionnaires de patronymes et de prénoms existants ainsi que des logiciels spécialisés pour attaquer toutes les combinaisons possibles de patronymes / prénoms ;

Dans le même ordre d'idées, aucun mot figurant dans un dictionnaire (noms communs ou noms propres ou noms d'animaux, pays, villes, régions, planètes...) ne doit être utilisé ;

- Il ne doit pas être constitué des mots de passe standards des constructeurs ;
- Il ne doit pas appartenir à des classes dont il est facile de tester l'intégralité des possibilités (plaques d'immatriculation des véhicules, dates...)[182].

Ainsi, pour conserver la confidentialité des données collectées, il est nécessaire pour ces réseaux de renforcer la robustesse des mots de passe des comptes. Ces mots de passe ainsi composés permettront de renforcer la sécurité de l'accès aux données enregistrées par les membres des réseaux sociaux.

La mise en place de la sécurité physique n'empêche pas la mise en place d'une sécurité logicielle.

B. La nécessité de prévoir une sécurité logicielle

La sécurité logicielle passe par la configuration des droits d'accès et d'habilitation des usagers (1). En outre, elle permet de se prémunir des failles applicatives (2).

1. La configuration des droits d'accès et d'habilitation des usagers

Il s'agit de filtrer l'accès aux données personnelles collectées. Ce filtrage se fait par la mise en place d'un dispositif de contrôle d'accès. Il sera donc associé à chaque usager un identifiant mnémonique ou physique. La mise en place d'un système de contrôle accès doit aussi respecter la loi portant protection des données à caractère personnel. La loi du 20 avril 2004 stipule que toute entreprise qui met en place puis gère un fichier automatisé de données nominatives est tenue de le déclarer[183].

Il faut noter que la configuration des droits d'accès et d'habilitation des usagers permet de restreindre l'accès aux serveurs des données et d'identifier les personnes qui y ont accès. Nous ne nous attarderons pas sur la restriction de l'accès aux données mais plutôt sur la capacité de ce dispositif à identifier les personnes en contact avec les serveurs des données.

---

[182] Assiste, Mot de passe : Un bon mot de passe, disponible sur « http://assiste.com/Mots_de_passe.html », (Consulté le 19 octobre 2018).

[183] Wikipédia, Vulnérabilité (informatique), disponible sur « https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9 », (Consulté le 19 octobre 2018).

Conformément aux dispositions de la loi portant protection des données personnelles, le responsable du traitement est tenu de garantir que puisse être vérifiée et constatée a posteriori l'identité des personnes ayant eu accès au système d'information contenant des données à caractère personnel.

Ainsi, ce dispositif sécuritaire permettrait aux responsables de traitement de remplir cette obligation. Cela participerait, par ailleurs, à une meilleure protection des données personnelles de leurs membres. Après une configuration des droits d'accès et d'habilitation des usagers, nous verrons comment prévoir les failles applicatives.

2. La prévention des failles applicatives.

Ce besoin répond la loi burkinabé relative à la protection des données personnelles qui dispose que le responsable du traitement est tenu de prendre toute précaution au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Il ressort, ici, que le responsable du traitement, dans les mesures qu'il devra mettre en place pour assurer la sécurité des données personnelles, doit prendre certaines précautions. Le traitement effectué étant un traitement automatisé, il doit donc se prémunir des failles applicatives. Les failles applicatives sont en réalité des vulnérabilités du système[184]. Pour définir le terme sur le plan informatique, il faut dire que c'est « une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient »[185]. Il est donc nécessaire de se prémunir de telles failles pour éviter de compromettre la sécurité des données personnelles collectées.

Ces failles qui sont des « portes entrouvertes » de façon volontaire ou non, peuvent faire l'objet d'attaques (les modes opératoires, les actions pirates). Ces attaques dépendent du but recherché : usurpation (manipulation de session) ; Introspection (injection : SQL, code) ; ou des failles : débordement, Formatage des chaînes, attaque brusque... Ces attaques peuvent entrainer la rupture de la « *triade DIC* », ce qui pourrait avoir un impact sur l'intégrité et la confidentialité des données collectées. Ces attaques peuvent par ailleurs, empêcher la disponibilité des

[184] Inecdot, interconnexion réseau et logiciel libre, disponible « https://www.inetdoc.net/guides/tutoriel-secu/tutoriel.securite.failles.html », (Consulté le 19 octobre 2018).

[185] Wikipédia, Vulnérabilité (informatique), disponible sur « https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9 », (Consulté le 19 octobre 2018).

données. Il est donc nécessaire d'anticiper ces failles dès la phase de conception, de spécification, de développement, ou de production pour la sécurité des données à caractère personnel collectées.

Après avoir faire un développement sur les mesures imputables aux compagnies de transports et MTOPO, nous analyserons dans le paragraphe suivant celles imputables aux utilisateurs.

Paragraphe II : Les mesures à prendre par les utilisateurs du téléphone mobile pour sécuriser leurs données à caractère personnel.

Pour mieux protéger leurs données personnelles, il est judicieux de montrer aux utilisateurs du téléphone mobile les risques et précautions liés à la protection de leurs données personnelles(A) et la sécurité des téléphones portables et chiffrement des mails(B)

A. Les Risques et les précautions liées à la protection des données personnelles dans l'utilisation des TIC.

Sous cette rubrique, nous envisageons d'informer, d'une part, les citoyens sur l'existence de risques liés à l'utilisation des TIC (1) et d'autre part, proposer des à cet effet, des conseils à suivre afin de minimiser les dits risques (2).

1. Les facteurs de risques liés à la protection effective des données à caractère personnel

Dans les téléphones mobiles, la conservation des sms envoyés transite sur le serveur SMS, et de ce fait ils sont conservés pendant une période plus ou moins longue ce qui peut entrainer une insuffisance de garantie de confidentialité et d'intégrité des sms[186]. En outre, la géolocalisation du téléphone permet de localiser avec exactitude la position géographique de son propriétaire, ce qui peut entrainer une intrusion dans sa vie privée et une perte de son intimité[187].

[186] Voir « www.cil.bf/conseils -pratiques- pour -une- meilleure -protection- des -personnelles », (consulté le 23/05/2019).
[187] Voir « https://.cnil.fr/maitrisez-les-les-reglages-vie-privee-de-votre-smaphone »,(consulté le 26/06/2019).

Dans la messagerie électronique (email), il y'a une insuffisance de sécurité en raison du fait que l'email ne garantit pas toujours la sécurité et la confidentialité des messages envoyés ou reçu à partir d'un terminal non -sécurisé.

L'adhésion des services de réseaux sociaux (Facebook, HI5, Twitter, Instagram, WhatsApp…) peut entrainer une exposition de la vie privée en raison que toute information donnée sur ce canal est souvent démultipliée[188]. Elle peut également entrainer une atteinte au droit à l'image parce que toutes les photos mises sur ce canal peuvent avoir plusieurs destinataires et être utilisées à d'autres fins à votre insu sans votre accord. L'adhésion à ces services peut porter une atteinte à la réputation parce que toute information ou photo transmise sur ce canal peut être utilisée ultérieurement en vue de salir votre réputation[189].

Les données personnelles peuvent être usurpées lorsque vous naviguez sur internet avec des ordinateurs non sécurisés ou lorsque vous installez des logiciels gratuits (freeware) ; des Peer to Peer (eMule, ares, limetier, etc.) sans précaution.

Il y'a également le risque de perte de données qui est le plus souvent causé par les virus informatiques qui peuvent corrompre ou supprimer des données de votre ordinateur.

Après avoir évoqué les facteurs de risques liés à la protection effective des données personnelles, nous donnerons des conseils pratiques pour une meilleure protection des données personnelles.

2. Les conseils et précautions pour une meilleure protection des données d'utilisateurs à caractère personnel

Les précautions élémentaires à prendre pour une utilisation sécurisée du courrier électronique[190] :

- Avant d'ouvrir un message électronique ou une pièce jointe, assurez-vous que votre antivirus est à jour ;
- Ne jamais transmettre des données confidentielles par messagerie électronique sans s'assurer de la sécurité du réseau ;
- Ne jamais répondre aux spams ou courrier électroniques qui demandent des renseignements personnels (mot de passe ou information financière) ;

[188] [188] Voir « www.cil.bf/conseils -pratiques- pour -une- meilleure -protection- des -personnelles »,(consulté le 23/05/2019)

[189] Ce que nous constatons sur les pages Facebook où leurs membres publient les informations personnelles sensibles de leurs amis sans leur consentement. Une meilleure sensibilisation doit être faite pour éviter les ces violations des droits des personnes concernées.

[190] Voir « www.cil.bf/a-telecharger- guide pdf », consulté le 02/02/2019.

- Activer le filtre anti-spam de votre logiciel de courrier électronique.

Pour les transactions en lignes notamment les opérations financières, il faut :

- Le faire uniquement chez des marchands dignes de confiance, pour cela il faut s'assurer que le site web est légitime, que l'adresse URL est exacte, y compris le nom de domaine ;
- S'assurer que le marchand se sert d'un système de transaction sécurisé. Pour s'assurer si un site web est sécurisé, s'assurer que le URL commence https:///ou shttps:// et qui apparait l'icône d'un cadenas verrouillé ou d'une clé intacte ;
- Après avoir effectué une opération financière ou bancaire en ligne, il convient de mettre fin à la session, vider la mémoire cachée et le fichier de témoins (cookies) ;
- Privilégier les sites qu'on a déjà fréquenté ou des sites recommandés[191].

Mesure et précautions à prendre lorsque vous utilisez les services de réseaux sociaux[192]

- Bien choisir quelles informations rendre visibles et avec qui les partager ;
- Ne pas accepter n'importe quelle invitation d'inconnu. On peut se retrouver en relation avec d'illustres inconnus, bien intentionné ou mal intentionné qui auront accès à nos données nominatives, email, numéro de téléphone, photos de famille ou d'amis, parcours scolaire, profession. Ces données personnelles peuvent être utilisées pour créer des messages d'hameçonnage, deviner votre mot de passe, usurper votre identité pour commettre éventuellement des infractions à votre insu ;
- Prendre le soin de configurer préalablement les paramètres de confidentialité ;
- S'appuyer sur la notoriété d'un éditeur avant d'intégrer un réseau social.

Avant de signer un contrat avec les éditeurs des logiciels de gestion ou de ses sous-traitants, l'utilisateur doit[193] :

- S'assurer que l'éditeur ou l'utilisateur à effectuer les formalités administratives préalables à la mise en œuvre des traitements ;
- S'assurer qu'il a mis en place des mesures organisationnelles et techniques à la protection de leurs données personnelles ;

[191] Idem
[192] Idem
[193]Les utilisateurs acceptent généralement les conditions d'utilisation des applications sans prendre le soin de les lire attentivement. Nous recommandons à ces derniers de les lire avant toute signature de contrat.

- Chercher à connaitre le niveau de protection de leur donnée par les responsables de traitements ;
- S'assurer du respect de la finalité des traitements des données ;
- Demander les procédures à suivre pour l'exercice de leurs droits ;
- S'assurer que les conditions d'utilisation des données personnelles sont effectives à une meilleure protection de leurs données. Après avoir évoqué les risques et précautions à prendre par les utilisateurs, nous verrons comment sécuriser les smartphones et chiffrement des mails.

B. La sécurité des téléphones portables et le chiffrement des mails

Sous cette rubrique, nous évoquerons d'une part les sécurisations contenues dans les téléphones (1) et d'autre part le chiffrement des mails (2)

1. Les sécurisations contenues dans les téléphones portables

Notre téléphone portable contient de plus en plus des informations (réseaux sociaux ouverts) nous concernant. En cas de perte ou de vol, des informations très personnelles peuvent être lues et rendues publiques.

Noter le numéro « IMEI » du téléphone.

Le code IMEI est le numéro de série unique composé de 15 à 17 chiffres identifiants votre téléphone. En cas de perte ou de vol, ce code sert à bloquer l'usage du téléphone sur les réseaux sociaux. Il est indiqué sur la boite du téléphone quand on l'achète. Notez-le et gardez-le en lieu sûr (pas sur le téléphone). On obtient le code IMEI en tapant *#06# sur votre téléphone[194].

Mettre en place un code PIN (Personnel Identification Numbers)[195]

Le code est un code secret qui contrôle la carte SIM quand on allume. Ce code verrouille le téléphone au bout de 3 codes erronés consécutifs. Il empêche l'utilisation de la carte SIM par une tierce personne, même avec un autre téléphone.

Mettre en place un code de verrouillage du téléphone[196]

[194] Ces informations sont issues de nos connaissances personnelles dans l'utilisation des smartphones
[195] Idem
[196] Idem

En plus du code Pin ce code permet de rendre inactif le téléphone au bout d'un certain temps. Cela empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol.

Ne pas accepter systématiquement la géolocalisation[197]

Certains téléphones permettent de situer le lieu où nous sommes. Il est possible de contrôler quand et par qui on peut être géolocalisé. Il suffit, pour cela, de régler les paramètres de géolocalisation du téléphone ou des applications de géolocalisation (twitter, Facebook, WhatsApp.). Il est également possible de désactiver ou de suspendre le service de géolocalisation à tout moment et de sélectionner les contacts qui sont autorisés à accéder aux données de localisation.

Les sécurisations contenues dans les téléphones portables nous amènent à montrer comment effectuer le chiffrement des mails.

2. La clé chiffrement de MAIL

Il s'agit d'un procédé, utilisant un certificat électronique personnel auto signée pour chiffrer ses mails appelés asymétrique[198]. Cela fonctionne d'une part avec une clé publique que vous pouvez communiquer à vos correspondants afin qu'ils chiffrent les emails qu'ils vous envoient. D'autre part, pour déchiffrer les mails reçus, vous avez besoin d'une clé privée qu'il faut garder secrète. Des logiciels libres tels que OpenGL, gpg4win, ainsi que les extensions pour Firefox et chrome (maivelope, firepgp) permettent de créer des paires de clés et de faire le chiffrement des mails sur le web mail.

Un meilleur moyen de protéger sa vie privée est de garder pour soi-même autant que possible les informations personnelles confidentielles.

[197] Voir «https://.cnil.fr/maitrisez-les-les-reglages-vie-privee-de-votre-smaphone »,(consulté le 26/06/2019).
[198] Dominique W. KABRE, Droit des technologies et de la télécommunication, op. cit. P. 45.

CONCLUSION

L'effectivité externe de la protection de la vie privée des citoyens peut être appréhendée dans deux (02) sens. Il s'agit dans un premier de leur conformité avec la loi portant protection des données personnelles. Dans un second, il faut se poser la question de savoir si les données personnelles ne sont pas réutilisées à d'autres fins sans le consentement des personnes concernées. C'est la problématique de la réutilisation des données personnelles à d'autres fins qui est visé dans ce second cas.

Au Burkina Faso comme dans la plupart des États africains, les différentes politiques en matière juridique étaient conçues dans le but de protéger la vie privée des personnes physiques et les données personnelles des personnes concernées. A l'époque, la politique de protection des données personnelles n'est pas souhaitable. En effet la CIL en tant qu'autorité indépendante en matière de protection des données personnelles connait beaucoup de faiblesse laissant subsister des intrusions à la vie privée. C'est à partir de 2004 que la question de la protection effective des données à commencer à intéresser les États d'Afrique.

Malgré la prise en conscience de la protection à travers l'adoption des législations spécifiques en la matière, elle n'arrive pas à parvenir à une meilleure protection des données personnelles des personnes concernées par le traitement. Par conséquent, la majorité des personnes concernées éprouve qu'elles soient victime des violations de leurs droits par les responsables des traitements. C'est pour cela que nous avons choisi de réfléchir sur le cas spécifique des voyageurs des compagnies de transport TSR et RAHIMO TRANSPORT.

Pour cela nous avons émis un certain nombre d'hypothèses considérées comme obstacle à la protection des données personnelles des voyageurs. Nous avons d'abord estimé que la principale source de la violation de la vie privée des voyageurs est le détournement de la finalité dès traitement des données personnelles autre que celle pour laquelle elles ont été collectées par les compagnies de transport. En outre, nous avons supposé que les entreprises qui collectent les données à caractère personnel des voyageurs ne les protègent pas efficacement. Par ailleurs nous avons estimé qu'il n'existe aucune relation entre les différentes entreprises dans le but de la protection des données à caractère personnel des voyageurs. Enfin les voyageurs ne sont pas informés de leurs droits à la protection des données collectées par les responsables des traitements.

Ce sont les résultats de nos enquêtes de terrain qui devaient confirmer ou infirmer ces hypothèses. Des questionnaires et des guides d'entretiens ont été distribués aux différents acteurs pour recueillir des données à cet effet. L'analyse de données recueillies a permis de procéder à la vérification de nos différentes hypothèses. En effet, 100% des personnes interrogées disent qu'elles ne sont pas informées de leurs droits sur la protection de leurs

données personnelles sur le logiciel CONEKTO TRANSPORT. Cela se justifie par le fait que les responsables du traitement et la commission n'informent pas les personnes concernées de leurs droits sur la protection de leurs données personnelles aggravant la réutilisation des données personnelles à d'autres finalités autre que la finalité initiale sans l'autorisation des personnes concernées. Cette situation vient confirmer notre hypothèse principale.

Les deux premières hypothèses secondaires selon lesquelles les entreprises qui collectent les données personnelles des voyageurs ne les protègent pas efficacement et qu'il n'existe aucune relation entre les différentes entreprises intervenant sur le logiciel CONEKTO TRANSPORT dans le but de la protection collective des données à caractère personnel des voyageurs ont été confirmées en ce que les enquêtes ont révélé que 100% des intervenants disent qu'ils n'existent pas une politique de gestion collective des données personnelles. Ce chiffre montre que les entreprises d'internet ou des responsables du traitement doivent mettre en place une politique de gestion collective des données personnelles de leurs membres.

La dernière hypothèse a trait à la méconnaissance des voyageurs de leurs droits à la protection des données collectées par les responsables des traitements a également été confirmée. Les dirigeants avec qui nous avons eu des entretiens affirment qu'ils n'ont pas informé les voyageurs de leurs droits sur la protection de leurs données personnelles et de la possibilité de les mettre en œuvre. Les personnes concernées méconnaissent l'existence d'une législation en matière de protection des données personnelles. Et donc cette hypothèse est également vérifiée.

Face à la protection ineffective des données personnelles des voyageurs nous avons eu à faire une proposition pour une meilleure protection des données personnelles des voyageurs. C'est ainsi que nous avons proposé une réadaptation de la LPDP et les mesures de sensibilisation des responsables du traitement des données personnelles et les personnes concernées. Nous avons ensuite proposé des précautions à prendre par les utilisateurs des smartphones, tablettes pour une protection de leurs données personnelles.

Cette étude n'a pas pour vocation de faire une analyse exhaustive de la protection des données personnelles des voyageurs sur les programmes d'ordinateurs.

BIBLIOGRAPHIE

A. Ouvrages

- BENSOUSSAN (A.), *Informatique, télécoms et internet*, 5 éd, Paris, Ed Lefebvre Francis, 2012, 1000 p.
- DESGENS-PASANAU (G.), *Protection des données à caractère personnel, Loi informatique et libertés*, 2 éd, Paris, Lexis Nexis, 2013, 294 p.
- FAUCHOUX (V.), DEPREZ (P.), BRUGUIERE (J-M.), *Le droit de l'internet : lois, contrats et usages*, 2 éd, Paris, LexisNexis, 2013, 419 p.
- CASTETS-RENARD, (C). *Droit l'Internet : droit européen et français*, 2e édit., Paris, Montchrestien ,2012.
- MATTATIA (F.), Loi et Internet : *Un petit guide civique et juridique*, 1ère éd, Paris, Ed EYROLLES, 2013, 234 p.
- RAY (J-E.), *Le droit du travail à l'épreuve des NTIC*, 1ère éd, Paris, Ed Liaisons, 2001, 247 p.
- DOCQUIR (B.), FESLER (D.), DEHARENG (E.), *Le Droit des nouvelles Technologies et de l'internet*, 2 éd, Paris, Ed Bruylant, 2012, 136 p.
- KABRE (D.W), *Droit des Technologies de l'Information et de la Communication*, 1ère éd. Janvier 2017, Burkina Faso, 165 p.
- MATTATIA (F.), *Le droit des données personnelles*, 2 éd, Paris, Ed EYROLLES, 2016, 234 p.
- MATTATIA (F.), *Internet et les réseaux sociaux : que dit la loi* ? 2 éd, Paris, Ed EYROLLES, 2016, 237 p.
- LARRIEU (J)., *Droit de l'internet*, Ellipses,2005.
- LE TOURNEAU, (Ph), *contrats informatiques et électroniques*, Paris, Dalloz,4e édi.,2006.

B. Thèses et Mémoires

- COULIBALY (I.), *La protection des données à caractère personnel dans le domaine de la recherche scientifique,* Thèse, Université de Grenoble, 2011, 1117 p.
- WALCZAK (N), *Protection des données personnelles sur l'internet*, France, 04 juillet 2014, p.1

- BEKARA (KD), *Protection des données personnelles coté utilisateur dans le e-commerce*, thèse, Institut National des Télécommunications, France, 2012, 229 p.
- Yaya(MS), *Droit de l'OHADA face au commerce électronique*, thèse, Université de Montréal et Université de Paris-Sud 11, France 2011, 219 p.
- KABRE (DW), *la conclusion des contrats par voie électronique : étude du droit burkinabé, à la lumière des droits européen, belge et français,* thèse, Faculté universitaires Notre Dame de la Paix (FUNDP) de NAMUR, Le harmattan,2013.
- Boto (MNE), *protection des données personnelles sur les réseaux sociaux : cas de la Cote d'Ivoire,* Université Catholique de l'Afrique de l'Ouest, Abidjan, ed.2017.
- Marie (L), *protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique,* Liège Université Library, France, HAL, éd.2018, 49 p.
- COUMET (C.), Données personnelles et réseaux sociaux, Mémoire, Université Paul Cézanne U III, 2008-2009, 85 p.
- KOUKOUGNON (E.), *Proposition d'adaptation de la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel en Côte d'Ivoire*, Mémoire, Université Catholique de l'Afrique de l'Ouest, 2014-2015, 94 p.
- ZAGBA (F.), *La protection du consommateur numérique en Côte d'Ivoire : cas de la téléphonie mobile, Mémoire,* Université Catholique de l'Afrique de l'Ouest, 2014-2015, 117 p

C. Rapports publics et séminaires

- Commission de l'Informatique et Libertés, rapport public de la CIL sur la protection des données personnelles, ed.2008,69 p.
- Commission de l'Informatique et Libertés, rapport public de la CIL sur la protection des données personnelles, ed.2010,63 p.
- Commission de l'Informatique et Libertés, rapport public de la CIL sur la protection des données personnelles, éd.2012,57 p.

C. Législation

- **Textes internationaux**

- Déclaration universelle des droits de l'homme du 10 décembre 1948.
- Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH) signée le 4 novembre 1950 à Rome par les Etats membres du Conseil de l'Europe et entrée en vigueur le 3 septembre 1953.

- l'Assemblée générale des Nations Unies Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée le 28 janvier 1981 à Strasbourg par le Conseil de l'Europe.
- Résolution 45/95 du 14/12/1990 de l'assemblé générale ONU
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adopté le 28 janvier 1981 par le Conseil de l'Europe.
- Convention européenne de droit de l'homme du 04 novembre 1950.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) adopté le 27 avril 2016 et rentra en vigueur le 25 mai 2018.
- Directive C/dir/1/08/11 du 19 Aout 2011 portant lutte contre la cybercriminalité dans l'espace CEDEAO
- Acte additionnel de la CEDEAO portant protection des données personnel
- Directive 95/46/CE du Conseil de l'Europe 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
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

➢ **Législations nationales**

- Loi n°010/AN du 20 Avril 2004 portant protection des données personnelles au Burkina Faso.
- Loi n° 045-2009/an portant règlementation des services et des transactions électroniques au Burkina Faso. jo n°01 du 07 janvier 2010
- Loi n°032-99/AN du 22 décembre 1999 portant protection de la propriété littéraire et artistique au Burkina Faso

➢ **Législation de droit comparé**

- Loi n°2004-801 du 06 aout 2004 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel de la France
- Loi ivoirienne n°2013-450 relative à la protection des données à caractère personnel

E. Sites internet

- www.cil.bf
- www.droit-technologie.org
- www.arcep.bf
- www.cnil.fr
- www.donneepersonnelle.fr
- www.juriscom.net
- www.legalis.net

D. Webographie

- COULIBALY (I.), La difficile appréhension du droit émergent des NTIC en Côte d'Ivoire, disponible sur «http://www.village-justice.com/articles/difficile-apprehension-droit,18339.html#SALiq0wsldgElWG7.99 »,(Consulté le 09 décembre 2018)

- DAGNAUD (M.), Les jeunes et les réseaux sociaux : de la dérision à la subversion, disponible sur « https://lectures.revues.org/11569 », (Consulté le 22/04/2019).
- Ligue des droits de l'Homme, Protection des données personnelles : Analyse comparée des législations et des pratiques dans neuf pays européens dans le contexte du cadre juridique européen, disponible sur « http://www.ldh-france.org/IMG/pdf/SynthesfrancaisFINALcorr-BD.pdf », (Consulté le 9 décembre 2018)
- Assiste, Mot de passe *:* Un bon mot de passe, disponible sur « http://assiste.com/Mots_de_passe.html », (Consulté le 19 octobre 2018).
- Wikipédia, Vulnérabilité (informatique), disponible sur « https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9 », (Consulté le 19 octobre 2018).

- Inecdot, interconnexion réseau et logiciel libre, disponible sur « https://www.inetdoc.net/guides/tutoriel-secu/tutoriel.securite.failles.html », (Consulté le 19 octobre 2018)
- Wikipédia, Vulnérabilité (informatique), disponible sur « https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9 », (Consulté le 19 octobre 2018) ;
- « www.cil.bf/conseils -pratiques- pour -une- meilleure -protection- des -personnelles », (consulté le 23/05/2019). ;
- https://.cnil.fr/maitrisez-les-les-reglages-vie-privee-de-votre-smaphone »,(consulté le 26/06/2019) ;
- Voir « www.cil.bf/a-telecharger- guide pdf », consulté (le 02/02/2019) ;

- https://.cnil.fr/maitrisez-les-les-reglages-vie-privee-de-votre-smaphone »,(consulté le 26/06/2019 à 17 h).

TABLE DES MATIERES

ANNEXES

Annexe 1 : Questionnaires et guides d'entretien

QUESTIONNAIRES 1

A l'intention des voyageurs des compagnies de Rahimo Transport, nous sollicitons des renseignements ci-dessous dans le cadre de nos recherches de fin de cycle à l'ESCO-IGES. Nous avons opté de réfléchir sur le thème : « ***Protection des données à caractère personnel sur les programmes d'ordinateurs au Burkina Faso*** : cas de MTOPO Payment Solutions, TSR et Rahimo Transport.

Nous vous remercions pour votre contribution.

I.**IDENTIFICATION DE L'ENQUETTE**

Nom……
……

Prénom(s)……
……

…...; Sexe……profession…….....

II. Motivation du choix du TSR

Question1 : vous avez choisi TSR en raison de :

- Sécurité lors du voyage ☐ respect des heures ☐ protection de votre vie privé ☐ efficacité dans la protection de vos données personnelles ☐ rapidité lors du voyage ☐

Autres (à préciser)
……
…….

Question 2 : connaissez-vous le niveau de protection de vos données personnelles ?

Oui ☐ non ☐

Justifiez votre reponse……
……
……
…….

III. Données personnelles

Question 1 : Quelles sont vos données collectées lors du paiement des tickets de voyage

Nom ☐ prénom ☐ numéro du téléphone ☐ email ☐

Si autre précise……

Question 2 : selon vous en quoi la collecte de ces données vous parait important ?

Evité la perte des tickets ☐ sécurité dans le transport ☐ lutte contre le terrorisme ☐

si autre precisez……

……
……
……

Question 3 : par quel moyen vos données sont- elles collectées ?

Ordinateurs ☐ tablettes ☐ autres ☐

Si autres préciser……

Question4 : Avez-vous une idée sur la protection des données personnelles ?

Oui ☐ non ☐

Si oui
laquelle ?.....
.....
.....

IV. moyen mis à la disposition des voyageurs dans le cadre de la Protection des données à caractère personnel.

Question 1 : savez-vous qu'il existe une législation en matière de protection de vos données personnelles au Burkina Faso ?

Oui ☐ non ☐

Si oui
laquelle……
……

Question 2 avez-vous déjà entendu parler d'une institution en matière de protection des traitements au Burkina Faso

Oui ☐ non ☐

Si oui
laquelle……
……

Question3-Etes-vous déjà été informés de vos droits sur la protection de vos données à caractère personnel ?

Oui ☐ non ☐

Si oui par quel moyen et par qui……
…….

Si oui lesquels des droits connaissez-vous ?

Droit d'opposition ☐ droit de rectification ☐ droit d'accès ☐ droit d'information ☐

Si autre préciser……
…….

Question4-Etes-vous sûr que l'exercice de ces droits vous permettes de protéger efficacement vos données personnelles

Oui ☐ non ☐

Sinon quelles sont vos suggestions pour assurer une meilleure protection des données personnelles au Burkina Faso.

……
……
…….**Merci pour votre contribution.**

Annexe 2: Questionnaires 2

A l'intention des voyageurs des compagnies du TSR, nous sollicitons des renseignements ci-dessous dans le cadre de nos recherches de fin de cycle à l'ESCO-IGES. Nous avons opté de réfléchir sur le thème : « ***Protection des données à caractère personnel sur les programmes d'ordinateurs au Burkina Faso*** **: cas de MTOPO Payment Solutions, TSR et Rahimo Transport.**

Nous vous remercions pour votre contribution.

I.IDENTIFICATION DE L'ENQUETTE

Nom……
……

Prénom(s)……
……

Age: ; Sexe……profession…….....

II. Motivation du choix du TSR

Question1 : vous avez choisi TSR en raison de :

- Sécurité lors du voyage ☐ respect des heures ☐ protection de votre vie privé ☐ efficacité dans la protection de vos données personnelles ☐ rapidité lors du voyage ☐

Autres (à préciser)
……
…….

Question 2 : connaissez-vous le niveau de protection de vos données personnelles ?

Oui ☐ non ☐

Justifiez votre reponse……
……
……
…….

III. Données personnelles

Question 1 : Quelles sont vos données collectées lors du paiement des tickets de voyage

Nom ☐ prénom(s) ☐ numéro du téléphone ☐ email ☐

Si autre précise……

Question 2 : selon vous en quoi la collecte de ces données vous parait important ?

Evité la perte des tickets ☐ sécurité dans le transport ☐ lutte contre le ☐ terrorisme

si autre
precisez……
……
……
……

Question 3 : par quel moyen vos données sont- elles collectées ?

Ordinateurs ☐ tablettes ☐ autres ☐

Si autres préciser……

Question4 : Avez-vous une idée sur la protection des données personnelles ?

Oui ☐ non ☐

Si oui
laquelle ?.....
.....
.....

IV. moyen mis à la disposition des voyageurs dans le cadre de la Protection des données à caractère personnel.

Question 1 : savez-vous qu'il existe une législation en matière de protection de vos données personnelles au Burkina Faso ?

Oui ☐ non ☐

Si oui
laquelle……
……

Question 2 avez-vous déjà entendu parler d'une institution en matière de protection des traitements au Burkina Faso

☐

Oui ☐ non

Si oui
laquelle……
……

Question3-Etes-vous déjà été informés de vos droits sur la protection de vos données à caractère personnel ?

Oui ☐ non ☐

Si oui par quel moyen et par
qui……
…….

Si oui lesquels des droits connaissez-vous ?

Droit d'opposition ☐ droit de rectification ☐ droit d'accès ☐ droit d'information ☐

Si autre
préciser……
…….

Question4-Etes-vous sûr que l'exercice de ces droits vous permettes de protéger efficacement vos données personnelles

Oui ☐ non ☐

Sinon quelles sont vos suggestions pour assurer une meilleure protection des données personnelles au Burkina Faso.

……
……
……**Merci pour votre contribution.**

GUIDES D'ENTRETIEN

Annexe 3 : Guide d'entretien 1

A l'adresse du Directeur du RAHIMO TRANSPORT. Nous vous sollicitons les informations ci-dessous dans le cadre de nos recherches de fin de cycle à l'ESCO-IGES. Nous avons opté de réfléchir sur le thème : « ***Protection des données à caractère personnel sur les programmes d'ordinateurs au Burkina Faso*** : **cas de MTOPO Payment Solutions, TSR et Rahimo Transport.**

Nous vous remercions pour votre contribution.

I.IDENTIFICATION DE L'ENQUETTE

Nom……
……

Prénom(s)……
……

Age:… Sexe……profession…….....

II. Finalité des traitements des données à caractère

Question 1 : Quelles sont les finalités de traitement des données de vos clients ?

Vente des tickets ☐ réservations tickets ☐ gestion des colis ☐

Question 2 : Avez-vous prévu d'autres finalités dans le traitement des données de vos clients ?

Oui ☐ non ☐

si oui
lesquelles……
……..

Avant la réutilisation des données avez-vous reçu le consentement de vos clients

Oui ☐ non ☐

II. Information des clients

Avez-vous informé aux clients leurs droits sur la protection des données personnelles ?

Oui ☐ non ☐

Si oui
lesquels……
……

Si oui par quel
moyen……
……

II. Mesures organisationnelles et techniques mise en place dans le cadre de la protection de données personnelles des clients.

Question1 : Quelles politiques avez-vous mis en place dans le cadre de protection des données ?

Politique de sécurité ☐ élaboration des identifiants aucun ☐

Question 2 : Avez-vous une politique de protection des données personnelles avec d'autre partenaire ?

Oui ☐ non ☐

Si oui préciser la
politique……
……
……

Quelles suggestions faites-vous pour une meilleure protection des données personnelles au Burkina
Faso…… ……
……
……
……
……
……
……
……
……

Merci pour votre participation

Annexe 4 : Guide d'entretien 2

A l'adresse du Directeur du TSR. Nous vous sollicitons les informations ci-dessous dans le cadre de nos recherches de fin de cycle à l'ESCO-IGES. Nous avons opté de réfléchir sur le thème : « ***Protection des données à caractère personnel sur les programmes d'ordinateurs au Burkina Faso*** : **cas de MTOPO Payment Solutions, TSR et Rahimo Transport.**

Nous vous remercions pour votre contribution.

I.IDENTIFICATION DE L'ENQUETTE

Nom……
……

Prénom(s)……
……

Age:……. Sexe……profession…….....

II. Finalité des traitements des données à caractère

Question 1 : Quelles sont les finalités de traitement des données de vos clients ?

Vente des tickets ☐ réservations tickets ☐ gestion des colis autres ☐

Question 2 : Avez-vous prévu d'autres finalités dans le traitement des données de vos clients ?

Oui ☐ non ☐

Si oui
lesquelles……
…….

Avant la réutilisation des données avez-vous reçu le consentement de vos clients

Oui ☐ non ☐

II. Information des clients

Avez-vous informé aux clients leurs droits sur la protection des données personnelles ?

Oui ☐ non ☐

Si oui
lesquels……
……

Si oui par quel
moyen……
……

II. Mesures organisationnelles et techniques mise en place dans le cadre de la protection de données personnelles des clients.

Question1 : Quelles politiques avez-vous mis en place dans le cadre de protection des données ?

Politique de sécurité ☐ élaboration des identifiants aucun ☐

Question 2 : Avez-vous une politique de protection des données personnelles avec d'autre partenaire ?

Oui ☐ non ☐

Si oui préciser la
politique……
……
……

Quelles suggestions faites-vous pour une meilleure protection des données personnelles au Burkina
Faso…… ……
……
……
……
……
……
……
……

Merci pour votre participation