LA PROBLÉMATIQUE DES DONNÉES PERSONNELLES TRANSMISES À L'OCCASION DE LA CONCLUSION D'UN CONTRAT : REGARDS CROISES DES JURISPRUDENCES MALIENNES ET FRANÇAISES

Dr. Sekoumarou DIABATE
Maitre-Assistant
Faculté de Droit Privé (FDPRI/USJPB), Bamako/ Mali.
diabatesekoumarou@yahoo.fr

RÉSUMÉ

La thématique proposée permet d'étudiée et d'établir les liens entre les données personnelles et le contrat, instrument privilégié des transactions économiques. En France, La Commission Nationale Informatique et Liberté (CNIL) qui est l'Autorité de protection des données a été confronté à la problématique des données bancaires des clients d'un site célèbre de commerce électronique : la conservation des cryptogrammes visuels des cartes bancaires dans une base consultable par les salariées de l'entreprise, expose les utilisateurs du site marchand, à un risque d'utilisation frauduleuse des données bancaires nonobstant la traçabilité des opérations mise en place. Et que des lors, l'entreprise de commerce électronique avait gravement manqué à l'obligation de sécurité et à l'obligation de confidentialité des données. Au Mali, l'Autorité de Protection des Données à caractère Personnel(APDP) considère dans sa Délibération n°2016-005 que l'accès de deux journaux aux factures non encore distribuées et non échues, ainsi qu'aux données client du plaignant au niveau de la SOMAGEP-SA et EDM-SA, constitue, de la part desdites sociétés, un manquement grave à l'obligation de sécurité et confidentialité qui leur incombe, tel que réprimé par l'article 65 de la loi n°2013-015 du 21 mai 2013. Ce sont ces aspects des données personnelles transmises lors de la conclusion d'un contrat que nous nous proposons d'analyser.

Mots clés. Droit, Culture numérique, Autorité Administrative Indépendante, Sécurité des données personnelles.

ABSTRACT

The proposed theme makes it possible to study and draw a link between personal data and the contract, a key instrument for economic transactions. In France, French Data Protection Authority - *Commission Nationale Informatique et Liberté* (CNIL), which is the Data Protection Authority, faced the issue of customers' account data of a famous e-commerce site: storage of visual cryptograms for bank cards in a database that can be consulted by company employees, exposes commercial website users to a risk of fraudulent use of bank data notwithstanding the traceability of the operations in place. And that henceforth, the e-commerce company

had seriously breached obligation of security and obligation of data confidentiality. In Mali, the Personal Data Protection Authority - *Autorité de Protection des Données à caractère Personnel* (APDP) considers in its Deliberation n°2016-005 that the access of two newspapers to invoices not yet distributed and not due, as well as to the complainant's customer data at the level of SOMAGEP-SA and EDM-SA, constitutes, from the said companies, a serious and repeated breach of obligation of security and confidentiality incumbent on them, as punishable under article 65 of law n°2013-015 of May 21, 2013. It is these aspects of personal data provided when signing a contract that we propose to analyze.

Key words: Law, Digital Literacy, Independent Administrative Authority, Security of Personal Data.

INTRODUCTION

Le droit des données personnelles[1] réglemente l›activité de traitement de données à caractère personnel. Cette activité, bien que concernant un certain nombre de tiers, oppose deux protagonistes essentiels : l›auteur d›un traitement de données personnelles et la personne fichée, dont les données font l›objet du traitement. Ce droit des données personnelles cristallise, cependant des enjeux importants qui trouvent à s'illustrer dans des questions concrètes et d'actualité[2]: les progrès technologiques, par exemple, augmentent notablement les risques d'atteintes aux droits et libertés fondamentales de la personne humaine de tels risques sont inhérents à l'usage de telles technologies, qui pourtant innervent notre quotidien. Dans ce contexte, la question se pose de l'efficacité des instruments relatifs aux données personnelles pour protéger les droits et libertés fondamentaux de la personne fichée relevant de l'initiative d'acteurs privés globaux. Pour certains, le cyberespace constituerait par nature une zone de non droit, rétive à une régulation juridique et étatique. L'internet, par exemple, a mis en avant le problème majeur de la traçabilité : toute connexion, toute consultation d'un site laissent des traces électroniques, collectées, rassemblées, traitées, diffusées, elles « parlent » de l'internaute qui devient transparent, elles diminuent ou suppriment la confidentialité des échanges. L'internaute laisse derrière lui volontairement et involontairement des « données-traces » que d'autres se chargent de collecter, d'interpréter, d'utiliser, de diffuser[3]. Ces considérations, trouvent leurs prolongements pratiques dans les différents incidents qui seront illustrés par les décisions des autorités ayant vocation à régir ces aspects du droit contractuelle des données personnelles comme l'APDP au Mali et la CNIL en France. Afin de mener à bien notre analyse sur la thématique proposée, nous suggérons d'étudier en premier lieu, la protection des données personnelles et les difficultés relatives à la formation du contrat **(I).** Et**,** en second lieu, la protection des données personnelles et les difficultés relatives à l'exécution du contrat **(II).**

1. LA PROTECTION DES DONNÉES PERSONNELLES ET LES DIFFICULTÉS RELATIVES A LA FORMATION DU CONTRAT

On examinera sous ce titre deux points essentiels, à savoir : en premier lieu, les difficultés susceptibles de surgir au moment l'échange des informations des contractants **(A)** et en second lieu, les difficultés à résoudre dans l'hypothèse de la rétractation du contractant **(B).**

A. L'ÉCHANGE D'INFORMATION

Une fois en transaction avec un fournisseur de service d'accès à internet, par exemple, et soumis à un contrat, l'utilisateur de communication électronique est contraint de dévoiler un certain nombre de données

[1] Constance CHEVALLIER-GOVERS, « Le droit à la protection des données à caractère personnel : un droit fondamental du XXI[ème] siècle ? », L'Harmattan, 2003, tome III, p. 79 et s.

[2] Conseil d'Etat, Le numérique et les droits fondamentaux, la Documentation Française, 2014.

[3] LUCAS André, DEVEZE Jean, FRAYSSINET Jean, Droit de l'informatique et de l'Internet, PUF, 2001, pp.14-15.

personnelles requises afin d'avoir accès au service. Sans pour autant savoir le sort réservé à ces données, une fois migrée de son poste. Le fournisseur de service électronique, selon un certain nombre de paramètres (son type, son secteur d'activité, ses objectifs, etc.) prétendra un usage défini, une durée de rétention délimitée et un certain nombre de moyens de protection des données personnelles ainsi acquises. Deux types de données sont stockées et gérées par les fournisseurs d'accès à internet : -Il s'agit premièrement les données fournies par l'utilisateur au moment de la souscription au service : -les données nécessaires à l'identification de l'usager ou du client voir du consommateur (nom, prénom, date de naissance, sexe, etc.) ; données nécessaires à la facturation du service (adresse de facturation et moyen de paiement) ; données complémentaires optionnelles que le fournisseur de services peut collecter pour un usage marketing à condition d'avoir obtenu l'accord explicite du client ; données complémentaires demandées en échange de la fourniture d'un service gratuit sur Internet.(historiques des navigations ; les sites et documents consultés, contenu des ,messages mails échangés) que le service utilise pour mieux connaître ses usagers ou financer ses activités. Il s'agit deuxièmement des données collectées pendant la fourniture du service. Il s'agit des données les plus sensibles en matière de vie privée. Ces données dépendent du type de service fourni : -tickets de facturation de retrouver l'ensemble des correspondant d'une personne (émission et réception) ; l'ensemble des sites web visités et des pages vues ; l'ensemble des lieux physiques ou un téléphone mobile allumé a été vue, même s'il n'a pas été appelé. Les services bancaires : l'ensemble des transactions de paiement horodatées avec les coordonnées de la contrepartie (commerçant) ; les incidents de paiements crédits et incidents de remboursement ; revenus récurrents. Les services de santé : informations sur les maladies d'une personne et les médicaments achetés. Les services d'éducation ; etc.

Il est à noter que de telles informations font l'objet de commerce lucratif entre les fournisseurs de services et d'autres partenaires de la sphère Internet. Ces utilisations sont de plus en plus contestées ; car elles sont faites en totale opacité, sans le consentement des utilisateurs. Elles génèrent des bénéfices substantiels souvent disproportionnées avec le service fourni. Les autorités administratives indépendantes veillent à la gestion et à la protection des données personnelles collectées et stockées par les structures concernées. Au Mali, l'autorité de protection des données à caractère Personnel (APDP) s'est prononcée sur la gestion et la protection des données personnelles collectées et stockées par les services fournisseurs : en vertu des dispositions de l'article 5 de la loi n° 2013-015 du 21 mai 2013 sont soumis à la loi susvisée, tous les traitements de données personnelles opérées sur le territoire malien par les organismes publics et privés. Au Mali, en vertu d'article 7 de la loi de 2013, le responsable de traitement est tenu de conserver sous une forme permettant l'identification des personnes concernées, les données pendant une durée qui n'excèdent pas celle nécessaire aux finalités pour lesquelles elles sont collectées ou utilisées. Au-delà de cette période le responsable de traitement est donc tenu d'effacer ou d'anonymiser les données[4].

En France par exemple, la Commission nationale de l'informatique et des libertés (dite CNIL) formule des recommandations aux entreprises en matière d'archivage. Du point de vue du régime juridique recommandé, la CNIL distingue trois hypothèses distinctes : les archives courantes, les archives intermédiaires, et les archives définitives. Le responsable de l'archivage doit donc mettre en place des techniques de conservation distincte selon la nature des données.

B. LA RÉTRACTATION DU CONTRACTANT

Le contractant en la personne du consommateur dispose de la faculté de rétractation et pour qu'il puisse en bénéficier de manière adéquate et l'exercer en toute connaissance de cause, l'existence de cette faculté doit lui avoir été communiquée. L'article 54 de la loi malienne de 2016, dispose en ce sens que : « avant que le consommateur ne soit lié par un contrat à distance ou par une offre, le professionnel fournit au consommateur, sous une forme claire et compréhensible sur le fond et sur la forme les informations suivantes : concernant le

[4] Voir en ce sens : Délibération n°2020-034 APDP du 12 février 2020 portant adoption du référentiel relatif aux mesures de sécurité et de confidentialité des données à caractère personnel.

droit de rétractation, l'existence d'un droit de rétractation ou l'absence d'un tel droit…, et le cas échéant, si le consommateur peut bénéficier d'un droit de rétractation , les conditions, le délai et les modalités d'exercice de ce droit…»[5]. Et l'article 72 de la même loi de 2016 d'ajouter que « le consommateur dispose d'un délai de quatorze (14) jours calendaires pour se rétracter d'un contrat à distance, sans avoir à motiver sa décision et sans avoir à supporter d'autres coûts que les frais directs de renvoi du bien »

Afin de permettre, par exemple, l'exercice de la faculté de rétraction la CJCE, dans un arrêt du 3 septembre 2009[6] refuse d'admettre que le consommateur ayant exercé son droit de rétractation soit redevable envers le professionnel d'une indemnité pour l'usage qu'il a eu du bien pendant le temps de sa réflexion. Cependant, si l'indemnité de jouissance est exclue, une indemnité compensatrice équitable est en revanche envisageable au profit du professionnel dans l'hypothèse où la déloyauté ou l'enrichissement sans cause du consommateur serait caractérisé. Dans la même logique la CJUE, dans un arrêt du 15 avril 2010[7] a souligné que la directive 97/7/CE sur les contrats à distance s'oppose à ce que le consommateur ayant exercé son droit de rétractation reste tenu de la charge des frais par lesquels la marchandise lui a été livrée. Le professionnel est donc tenu de rembourser les frais de l'expédition initiale avec le prix qu'il avait reçu.

Le droit de rétractation connaît toutefois de nombreuses limites qu'il convient de relever. L'article 75 de la loi malienne de 2016 relative aux transactions, échanges et services électroniques précise en ce sens que le droit de rétractation est exclu en ce qui concerne plusieurs types de contrats, cet article 75 de la loi de 2016, recense pas moins de 12 types de contrats : La fourniture de boissons alcoolisées dont le prix a été convenu au moment de la conclusion du contrat de vente, dont la livraison ne peut être effectuée qu'après trente (30) jours et dont la valeur réelle dépend des fluctuations du marché échappant au contrôle du professionnel ; 8. La fourniture d'enregistrement audio ou vidéo scellés ou de logiciels informatiques scellés et qui ont été descellés après livraison ; 9. La fourniture d'un journal, d'un périodique ou d'un magazine sauf pour les contrats d'abonnement à ces publications ; Les contrats conclus lors d'une enchère publique ; La prestation de services d'hébergement autres qu'à des fins résidentielles, de transport, de location de voitures, de restauration ou de service lié à des activités de loisirs si le contrat prévoit une date ou une période d'exécution spécifique ; La fourniture d'un contenu numérique non fourni sur un support matériel, si l'exécution a commencé avec l'accord préalable express du consommateur ou si un moyen fonctionnellement équivalent au droit de rétractation permet de garantir le consentement du consommateur avec la même efficacité, le consommateur ayant pris acte qu'il perdrait son droit de rétractation.

En ce sens, également, la jurisprudence française, rappelle que de nombreuses limites s'imposent en ce qui concerne l'exercice de la faculté de rétractation.

En France, le juge de proximité de Dieppe, dans un jugement du 7 février 2011[8] a rappelé à l'occasion, de l'achat d'un robot mixeur effectué par un particulier auprès d'un autre particulier que le droit de rétractation de l'article L. 121-16 du Code de la consommation française ne concerne que le contrat de vente à distance conclu par un consommateur avec un vendeur professionnel. La Cour de cassation française a eu elle aussi, l'occasion de préciser que : le droit de rétractation ne s'applique pas aux contrats conclus par voie électronique ayant pour objet la prestation de services d'hébergement, de transport, de restauration, de loisirs. Un couple avait réservé sur Internet un voyage pour le mois suivant par l'intermédiaire de l'agence Go Voyages après avoir repéré une erreur de rétractation pour les voyages en ligne. La Cour de cassation française avait déjà par le passé décidé l'exclusion de ce droit de rétractation pour l'achat par Internet d'un billet de chemin de fer[9].

---

[5] Article 54 de la loi n° 2016-12/ du 6 mai 2016 relative aux transactions, échanges et services électroniques en République du Mali.

[6] CJCE 1re ch., Aff. C-489/07, Pia MESSNER c/ Firma Stefan KRUGER.

[7] CJUE. Affaire C-511/08, HANDELGESELLESCHAFT Heinrich Heine.

[8] TI Dieppe, jur. Proximité ; 7 févier 2011, Igor D. c/ Priceminister www.legalis.net

[9] C.Cass. 1re civ.,6 décembre 2007, n° du pourvoi : 0616.466

2. LA PROTECTION DES DONNÉES PERSONNELLES ET LES DIFFICULTÉS RELATIVES A L'EXÉCUTION DU CONTRAT

Seront étudiés sous ce titre deux points également importants. Le premier point traitera des types de contrats concernés **(A)**. Tandis que le second point abordera la question de responsabilités engagées lors de l'exécution du contrat **(B)**.

A. LES CONTRATS CONCERNES

Selon le contexte géographique indiqué des deux pays cités en exemples dans cette étude que sont la France et le Mali. Nous nous attacherons à présenter les décisions des autorités juridictionnelles respectives concernées que sont celles de la Commission Nationale de l'Informatique et des Libertés **(CNIL)** pour la France **(1)** et celles de l''Autorité de Protection des Données Personnelles **(APDP)** pour le Mali **(2)**.

1. LE CONTEXTE DE LA JURISPRUDENCE EN FRANCE : LES DELIBERATIONS DE LA CNIL

Il s'agit ici de répertorier les décisions rendues par la CNIL française Autorité Administrative Indépendante (AAI) qui fait office de juridiction de 1er degré avec possibilité d'exercer directement un recours devant le Conseil d'État. En matière de données personnelles transmises à occasion de la conclusion d'un contrat. Nous proposons ainsi de passer en revue trois types de contrats

a) Société d'Équipement Nord Picardie, Contrat de travail, accident de travail et géolocalisation (délibération n° 2012-213 du 22 juin 2012 portant sanction pécuniaire à l'encontre de la société Équipements Nord Picardie)

Une société spécialisée dans l'adduction et le traitement de l'eau assure pour le compte des collectivités territoriales des interventions de maintenances sur les réservoirs d'eaux desservant les populations. Suite à un accident de la circulation survenu durant sa période d'emploi un salarié en contrat à durée déterminée a souhaité accéder aux données à caractère personnelle figurant dans son dossier et spécialement aux données de géolocalisation concernant le véhicule de service qu'il utilisait le jour de l'accident. La demande visait à faire reconnaître par le Tribunal des affaires sociales, le caractère d'accident du travail de cet accident de la route. En effet, ce litige porte sur la reconnaissance du caractère professionnel de l'accident de la circulation subi par le plaignant, que l'analyse des données de géolocalisation permettra d'établir. La demande formulée auprès de son employeur s'étant avérée infructueuse, le salarié concerné a déposé une plainte auprès de la Commission nationale de l'informatique et des libertés (ci-après la « CNIL » ou la « Commission » le 23 juin 2011. Le 1er juillet 2011, la Commission a ainsi adressé à la société un courrier l'enjoignant de présenter ses observations et les mesures adoptées pour répondre à la demande d'accès et de communication des informations à caractère personnelles détenues par la société. Constatant la persistance de la non-communication des données demandées au plaignant, la Présidente de la Commission a adopté, le 16 décembre 2011 une décision mettant en demeure la société, sous quinze jours : -de communiquer au plaignant l'ensemble des données personnelles détenues dans l'ensemble des traitements de la société, et en particulier les données collectées par le système de géolocalisation mis en place sur son véhicule ; - de lui communiquer les procédures mise en place pour répondre aux demandes formulées en application de **l'article 39 de la loi française du 6** janvier 1978, s'agissant notamment du droit d'accès des employés aux données les concernant. En réponse à la mise en demeure, la société a, le 4 janvier 2012 adressé un courrier à la Commission lui indiquant la possibilité d'une consultation sur place, par le plaignant des informations demandées, mais refusant de lui en communiquer une copie. Par courrier du 12 janvier 2012, la Commission a adressé un courrier à la société lui rappelant les obligations lui incombant en application de l'article 39 de la loi précitée**.**

b) Contrat de vente relatif à des achats effectués sur le web : Société Optical Center (délibération SAN-2018 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société)

La société en question ici est spécialisée dans le commerce de détail d'optique. Elle dispose à cet effet d'une centaine de succursales, d'un réseau de 410 franchises et d'un site internet. Elle pressentait pour l'année 2016 un chiffre d'affaires consolidées d'environ 193 millions d'euros, le chiffre d'affaires généré par son site internet s'élevant à près de 4,25 millions d'euros. Le 28 juillet 2017, la Commission nationale de l'informatique et des libertés (CNIL France) a été informée d'une possible fuite de données concernant la société X. ce signalement faisait état de données personnelles rendues librement accessibles à partir de plusieurs URL qui lui avaient transmises , à plusieurs factures contenant des données personnelles suivantes: nom, prénom, adresse postale, correction ophtalmologique et, pour certaines d'entre elles, la date de naissance des clients ainsi que leur numéro d'inscription au répertoire national d'identification des personnes physiques (NIR). L'article 34 de la loi française du 6 janvier 1978 modifiée dispose que le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Ce second cas est relatif au défaut de sécurisation de l'accès à des bases de données. Les données étaient accessibles, sans procédure d'authentification sur des adresses URL du site de la société X. Les informations concernées notamment les suivantes : nom, prénom, adresse postale, correction ophtalmologique et, pour certaines d'entre elles, la date de naissance des clients ainsi que leur numéro d'inscription au répertoire national d'identification des personnes physiques. Des factures et des bons de commandes relatifs à des achats passés sur le site étaient également impliqués. Bien que la faille ait été ultérieurement corrigée, les données en cause sont restées accessibles pendant plusieurs semaines. Le défaut tenait à l'absence de procédure d'authentification des clients avant de leur permettre l'accès aux documents les concernant. Aussi la CNIL française a-t-elle décidé dans sa délibération du 7 mai 2018 de sanctionner la société Optical Center en lui infligeant une sanction pécuniaire de 250000 euros.

c) Contrat de connexion et service de transport sur le web : Société Uber (Délibération n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Uber)

La société Uber pour activité le transport des personnes avec chauffeur, dit VTC, via une plateforme web et une application mobile. Afin de proposer ce service dans d'autres pays, plusieurs filiales ont été créées dans le monde. La société compte environ 16000 salariés. En 2017, elle a réalisé un chiffre d'affaires d'environ 6 milliards d'euros. Le 21 novembre 2017, la société a publié sur son site un article faisant état de ce que qu'à la fin de l'année 2016, deux individus extérieurs à la société avaient accédé aux données de 57 millions d'utilisateurs des services à travers le monde. Le 28 novembre, la succursale française de la société Uber a adressé un courrier à la présidente u groupe de travail de l'article 29 sur la protection des données, l'informant des circonstances de la violation de données et de sa volonté de coopérer avec toutes les autorités compétentes sur cette affaire.

Un questionnaire portant sur les circonstances de la violation de données et sur les mesures prises est adressé par la CNIL France à la société. Ce troisième exemple tiré de la jurisprudence française est également relatif à la sécurité des données. Les textes législatifs définissent ainsi le responsable de traitement comme la personne qui seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données il faut ici aussi se référer à article 34 de la loi française du 6 janvier 1978 précité. C'est en ce sens que la société Uber s'est vu infliger une sanction pécuniaire de 400.000 euros pour ne pas avoir su prévenir une intrusion malveillante dans ses bases de données, (Cybercriminalité ou Cyber attaque). (Délibération du Cnil du 19 décembre 2018) La société Uber a en effet négligé de prendre certaines précautions qui auraient permis de prévenir une attaque informatique.

2. LE CONTEXTE DE LA JURISPRUDENCE AU MALI : LES DELIBERATIONS DE L'APDP

Il s'agit ici des décisions rendues sous la forme de délibérations par l'autorité Administrative Indépendante (AAI) malienne en la matière il s'agit : de l'APDP, autorité juridictionnelle de premier et dernier degré avec possibilité de recours contre ses délibérations devant la chambre administrative de la Cour Suprême du Mali. Quatre types de contrats, ayant fait l'objet de traitement par l'Autorité malienne seront également proposé à l'analyse sous ce titre.

a) Contrat client BICIM

Le 24 mars 2016, la Banque Internationale pour le Commerce et l'Industrie au Mali (BICIM) a saisi l'APDP, pour une demande d'autorisation de transfert de données personnelles des clients américains, en vue de les communiquer à l'administration fiscale américaine. En effet, en application de la loi américaine FATCA (Foreign Account Tax Compliance Act), adoptée en 2010 par le Congrès américain, le gouvernement des États-Unis d'Amérique demande aux institutions financières étrangères que, les données des clients américains soient communiquées à l'administration fiscale américaine, en vue de lutter contre la fraude et l'évasion fiscales. Il ressort de la demande, que le traitement envisagé a pour finalité « la gestion des clients qui présentent des indices d'américanité dans le cadre de la déclaration (FATCA). Conformément aux articles 7 et 57 de la loi malienne du 21 mai 2013 portant protection des données personnelles l'APDP note que la finalité est définie, explicite et conforme à l'avis du Ministre en charge de l'économie et des finances du Mali. Il ressort du dossier, que les données traitées portent entre autres, sur le nom, l'adresse des clients concernés, le NIF américain, leurs numéros de compte, ainsi que le solde des dits comptent. Le principe de consentement préalable, requis pour la communication des données étant respecté ; la BICIM à identifier les clients concernés et à transférer les données personnelles. (Délibération n° 2016-004/APDP du 16 août 2016 relative à la demande d'autorisation de la BICIM portant sur le transfert des données personnelles à l'administration fiscale américaine).

b) Contrat client EDM-SA et SOMAGEP-SA

Le 20 juin 2016 l'APDP est saisie d'une plainte contre la SOMAGEP-SA et l'EDM-SA pour communication illicite des données personnelles d'un client visant à porter atteinte à l'honneur et à la considération de celui-ci en violation des dispositions l'article 65-1 de la loi du 21 mai 2013 portant protection des données personnelles au Mali. A l'appui de sa plainte, le conseil du plaignant expose que le lundi 23 mai 2016, les factures d'électricité et d'eau du mois d'avril de son client ont été publiées à la « Une » de deux journaux avec en page intérieure l'affirmation que le sieur devait plusieurs millions de redevances aux deux sociétés. Que la même « Une » circulait déjà sur les réseaux sociaux. L'article 8 de la loi malienne de 2013 dispose que « le responsable du traitement prend toutes les précautions utiles pour préserver la sécurité des données. Il doit empêcher notamment qu'elles soient déformées, endommagées ou que des tiers non autorisés y accèdent ». En déclinant toute responsabilité dans la transmission des données du sieur aux journalistes, les deux sociétés mises en cause, EDM-SA et SOMAGEP-SA ont toutes deux dans leurs mémoires en défense, déploré la publication des données de facturation du plaignant dans des organes de presse. L'autorité de protection des données à caractère Personnel (APDP), après en avoir délibéré conformément à la loi, déclare EDM-SA et SOMAGEP-SA responsables de la violation de **l'article 8 de la loi de 2013**. Et l'autorité malienne des données a ainsi prononcé à l'encontre de la SOMAGEP-SA une amende de 5.000.000 de francs CFA. Et contre EDM-SA une amende de 5.000.000 de francs CFA. (**Délibération n° 2016-005/APDP relative à la plainte pour atteinte à la vie privée...**).

c) Contrat de travail et caméra de vidéo-surveillance

La société Escort Sécurité Privé, est une entreprise commerciale de droit malien œuvrant dans le secteur de la sécurité privée. Dans le cadre de ses activités, elle emploie des vigiles déployés sur le terrain et des opérateurs chargés de leurs surveillances. Le 27 avril 2020 un des employés de l'entreprise a saisi le

Président de l'APDP d'une plainte contre la société Escort Sécurité Privée et son directeur Général pour atteinte à ses données personnelles en violation des dispositions de l'article 68 de la loi malienne du 21 mai 2013 portant protection des données personnelles. A l'appui de sa plainte, l'employé a exposé, que ladite société a fait installer des caméras de surveillance dans tous ses bureaux, que récemment il a été congédié verbalement par le directeur sur la base d'images issues de ce système de vidéo-surveillance, qui s'est révélé illicite à la suite de la consultation du répertoire de traitements des données de l'APDP. Il a estimé que cela est contraire aux disposition de l'article 68 de la loi portant protection des données personnelles en République du Mali qui dispose : « les services publics et les personnes physiques ou morales dont l'activité consistait, la date de promulgation de la présente loi à effectuer, à titre principal ou accessoire, des traitements de données personnelles disposent d'un celai maximum de six (6) mois, pour se conformer aux disposition de la présente loi », c'est pourquoi il porte plainte contre la dite société pour installation illicite du dispositif de vidéo-surveillance et détention illégale de fichier audiovisuel par son employeur pour fin d'intimidation et de pression à l'encontre de sa personne. Suivant l'ordre de mission n° 2020-021 du 4 mai 2020, une mission de l'APDP a effectué le 05 mai 2020, un contrôle au niveau de ladite société de son dispositif de vidéo-surveillance. La mission de l'autorité a constaté les manquements suivants aux normes de protection des données personnelles en matière de mise en place de système de vidéo-surveillance : la non déclaration du système, le non-respect de l'obligation de consultation des représentants du personnel, la non précision de la finalité du traitement, la disproportionnalité entre la finalité annoncée et les emplacements des caméras ; le non-respect des droits des personnes concernées. Ces différents manquements entachent la licéité de l'article 7 de la loi du 21 mai 2013 et pouvaient donner lieu à l'application des sanctions prévues à cet effet. (Délibération n° 2021-015/APDP du 09 février 2021 portant sanction de la société Escort Sécurité Privée).

d) Contrat de société Supermarché « SHOPREATE Libre-Service »

Une délégation de l'Autorité de Protection des données a effectué, les 14 et 15 mai 2020 auprès du supermarché SHOPREATE Libre-service une mission de contrôle de conformité de son dispositif de vidéosurveillance. La délégation de l'Autorité a constaté les manquements suivants aux normes de protections des données personnelle en matière de mise en place de système de vidéosurveillance : -La non déclaration du système de vidéosurveillance à l'APDP ; -le non-respect de l'obligation de consultation des représentants du personnel ; -la non-précision de la finalité du traitement ; -le non-respect des droits des personnes concernés (salariés, client, visiteurs) ; -le non-respect de la durée de conservation des images collectées. Ces faits ainsi relevés constituent des violations des règles de fond et de formes posées par la loi malienne du 21 mai 2013, ainsi que de la délibération n° 2017-024/APDP du 11 avril 2017 portant sur les conditions de mise en place de système de vidéosurveillance sur les lieux privés et les lieux de travail. L'autorité avait mis en demeure le Supermarché, sous un délai d'un mois, à compter de la notification de la délibération de procéder à l'accomplissement des formalités préalables applicables aux traitements mise en œuvre…

B. LES RESPONSABILITES ENGAGEES

Deux points seront examinés ici : il s'agit premièrement de l'étude de la violation des règles de formes et fonds des normes de protection des données personnelles (le fait générateur de la faute) **(1)** et deuxièmement de l'étude des sanctions prévues par les normes de protection des données personnelles **(2)**.

1. LA VIOLATION DES REGLES DE FORMES ET DE FOND DES NORMES DE PROTECTION DES DONNEES PERSONNELLES

a) S'agissant de la violation des règles de formes -Sur la qualité de responsable de traitements :

L'article 3-1 de la loi française du 6 janvier 1978 modifiée dispose que le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les disposition législatives et réglementaires

relative à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. Et l'article 5-1 de la même loi d'ajouter que sont soumis à la présente loi les traitements de données à caractère personnel : dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique… Au Mali, en vertu de l'article 5 de la loi malienne de 2013 (modifiée) sont soumis à la loi susvisée, tous les traitements de données à caractère personnel opérés sur le territoire malien par les organismes publics et privés. Au regard de ces dispositions, le droit applicable dépend de deux conditions cumulatives : l'existence d'un établissement du responsable de traitement sur le territoire et la mise en œuvre du traitement de données dans le cadre des activités de cet établissement. **Concernant le défaut de déclaration du traitement à l'APDP :** Le défaut de formalités préalables, comme la non déclaration du dispositif de vidéo surveillance auprès de l'autorité en violation des articles 33 et 57 de la loi de 2013. Ainsi que le défaut d'information des personnes concernées. L'article 57 de la loi 2013, dispose, par exemple que les responsables de traitement de données déclarent à l'Autorité de Protection les opérations qu'ils comptent effectuer pour une finalité donnée. Si cette formalité a été omise de mauvaise foi, l'autorité de Protection inflige au responsable de traitement des données en cause ; la sanction administrative appropriée qu'elle apprécie en fonction de la gravité de la faute[10].

b) S'agissant de la violation des règles de fond.

Il peut s'agir par exemple de la non précision de la finalité du traitement du non-respect du droit d'accès des personnes concernées, du non -respect du délai de conservation des données. **Concernant la non précision de la finalité du traitement. Violation de règles de fond :** l'article 7 de la loi française de 1978 modifiée, dispose que tout traitement de données à caractères personnel doit être effectué sur la base d'une finalité déterminée, explicite et légitime. Il ressort du dossier que l'équipe de contrôle n'a eu accès à aucun document précisant la finalité du traitement mis en œuvre ; que faute d'élément concret (réponse évasive), qui leur a été simplement dit que le système de vidéo-surveillance mis en place a pour finalité la sécurisation des personnes et des biens. (Cas de la délibération CNIL portant sanction pécuniaire à la Société Équipement Nord Picardie). **Relativement au manquement à l'obligation d'assurer la sécurité et la confidentialité des données** (cas de la société Optical center): l'article 34 de la loi française du 6 janvier 1978 modifiée dispose que le responsable du traitement est tenu de prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y est accès. Le manquement constaté à cette obligation donne lieu à sanction après mise en demeure par la Commission : ainsi dans le cas de la société Optical center, la commission française de la CNIL considère par exemple dans sa délibération que le manquement à l'article 34 est constitué dès lors que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées[11].

2. LES CONSEQUENCES DE LA VIOLATION DES NORMES DE PROTECTIONS DES DONNEES : LES SANCTIONS PRONONCEES

L'autorité de contrôle dispose d'un pouvoir de contrôle important en la matière, pouvoir corrélé à un pouvoir de sanction en cas de violation des normes de protection des données personnelles. Les sanctions visent à assurer le respect des obligations règlementaires ainsi qu'à inciter à l'adoption de mesure correctrices. Différentes sanctions peuvent être prononcées sous couvert du respect d'une mise en demeure préalable et des droits de la défense : Par exemples, les contrevenants à **l'article 56 de la loi malienne de 2013** s'expose ainsi à des **sanctions pénales : amendes, emprisonnement, retrait ou suspension de la licence d'exploitation. C'est en ce sens que l'autorité de contrôle peut dénoncer devant le Procureur de la**

[10] Pour la CNIL française cf. article 21 de la loi du 6 janvier 1978 dite « informatique et libertés »

[11] Cf., pour le Mali : article 8 de la loi de 2013.

République tout usager en infraction vis-à-vis de la loi sur les données personnelles. Les contrevenant à **l'article 61 de la loi malienne de 2013**, s'expose à des **sanctions administratives** : avertissement à l'encontre du responsable de traitement de données qui n'a pas observé les formalités administratives de collecte de traitement et de gestion des données prévues par la loi de 2013, l'injonction de cesser les activités de traitement des données personnelles ; le retrait d'agrément à tout responsable de traitement de données… Sont punis, au titre de **l'article 65 de la même loi malienne de 2013** d'une amende de cinq millions (5.000.000) à vingt millions de francs CFA : le fait de communiquer à des tiers non autorisés des données personnelles mettant en cause les droits fondamentaux et la vie privée ; le détournement de finalité d'une collecte ou d'un traitement de donnée personnelle, sans autorisation express ou motivée de l'Autorité de Protection des Données personnelles [12].

CONCLUSION :

L'étude cherchait à apporter un éclairage pratique sur l'application des lois sur les données personnelles dans les secteurs du droit des affaires et économiques. En effet, l'informatique et les réseaux sociaux favorisent la libre circulation des informations, dans ce contexte, la loi a pour but de veiller à ce que les préoccupations économiques et financières ne l'emportent pas sur la préservation des droits fondamentaux des personnes : en ce sens, c'est seulement depuis 2013 que le Mali dispose d'un cadre juridique portant sur la protection des données à caractère personnel. Tandis qu'en France, c'est depuis 1978, que la loi Informatique et liberté sur la protection des données personnelles des personnes a été promulguée. En définitive, l'appréhension imparfaite de la réalité contractuelle et de sa diversité (les limites du formalismes et l'existence des contrats d'adhésion) laissent penser que l'usage du contrat par le droit des données personnelles négligent certaines des spécificités de l'instrument utilisé.

BIBLIOGRAPHIE :

- **Autorité de protection des données à caractère personnel (APDP),** Recueil des normes et des délibérations de l'APDP. Bamako, République du Mali, Aout 2021. p. 3 à 64.
- **Commission Nationale de l'Informatique et des Libertés (CNIL),** « Recommandations pour les entreprises, 2012. p.1 ets.
- **France Loi n°2004-801 du 6 aout 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 aux libertés.
- **Mali. Loi n° 2016+-012/ du 6 mai 2016 relative aux transactions, échanges et services électronique en République du Mali ; Loi** n°2013-015 du 21 mai 2013 modifiée portant protection des données à caractère personnel en République du Mali.
- **MOLLO Fabrice** ., « La notion de données à caractère personnel », in Les sciences sociales et leurs données, Rapport au Ministre de l'Education Nationale, R. SILBERMAN, juin 1999, Annexes juridiques, p. 172 http://education.gouv.fr/rapport/silberman/table.htm **.**
- **SOW Djibril**, L'adaptation du droit des contrats au numérique, RCDA, n° 1, Janv-Mars 2013 p. 5 et s.

[12] Cf. Pour la France loi du 6 janvier 1978 dite Informatique et liberté : les sanctions de la CNIL vont aussi de la simple mise en demeure jusqu'aux sanctions financières (jusqu'à 300 000euro d'amende) et la publication dans la presse de ces sanctions au frais du sanctionné. Cf. aussi article 226-16 et suivants du Code pénal.