La responsabilité des entreprises en matière de protection des données personnelles à l'aube de l'actuelle transformation numérique au Maroc

Zineb MELLOUKI

Doctorante en Droit des affaires. Laboratoire de recherche : Droit, philosophie et société (ESSOR), Faculté des sciences juridiques, économiques et sociales, Université Sidi Mohamed Ben Abdellah, Maroc

Bouchta ALOUI

Professeur à la Faculté des sciences juridiques, économiques et sociales, Université Sidi Mohamed Ben Abdellah, Maroc

Résumé:

A nos jours, le Maroc expérimente une expansion numérique rapide dans divers secteurs. Une notion à laquelle beaucoup d'attention fut consacré ses dernières années, étant donné les vastes opportunités qu'offre ce modèle de développement pour ses adhérents. Ainsi, dans un tel paysage numérique, qui est en constante évolution, un encadrement juridique solide se voie indispensable pour garantir la sécurité lors de l'adoption de ce mécanisme, de telle sort que cela ne heurte la confidentialité et la protection des données à caractère personnel et plus précisément les données personnelles engageants la responsabilité des entreprises.

En effet, les organismes sociétaux vivent actuellement une prolifération des transactions en ligne, des plateformes digitales et de la collecte de données à grande échelle, qui soulèvent la question de la confidentialité des informations personnelles, qui devint une préoccupation majeure pour le législateur.

Abstract:

Morocco has recently experienced a rapid digital expansion across various sectors, presenting vast opportunities while necessitating a robust legal framework to ensure the security and confidentiality of personal data. Indeed, the proliferation of online transactions and large-scale data collection has raised significant privacy concerns, making the legal protection of personal data crucial. It is for this reason that the Moroccan legislator has undertaken substantial reforms to enhance the country's economic attractiveness, particularly by regulating and protecting the digitalization process.

Introduction :

A nos jours, le Maroc expérimente l'expansion fulgurante du digital au sein de ses divers départements. Une notion à laquelle beaucoup d'attention fut consacré ses dernières années, étant donné les vastes opportunités qu'offre ce modèle de développement pour ses adhérents. Ainsi, dans un tel paysage numérique, qui est en constante évolution, un encadrement juridique solide se voie indispensable pour garantir la sécurité lors de l'adoption de ce mécanisme, de telle sort que cela ne heurte la confidentialité et la protection des données à caractère personnel et plus précisément les données personnelles engageants la responsabilité des entreprises.

En effet, les organismes sociétaux vivent actuellement une prolifération des transactions en ligne, des plateformes digitales et de la collecte de données à grande échelle, qui soulèvent la question de la confidentialité des informations personnelles, qui devint une préoccupation majeure pour le législateur. Ainsi, l'ère actuelle du numérique, où les données personnelles sont devenues une monnaie d'échange inestimable, la sécurité juridique de ces informations sensibles s'avère cruciale, d'un côté, Face aux avancées technologiques qui continuent d'accélérer et d'un autre, face à l'émergence des entreprises dans leurs transactions numériques.

De ce fait, La confiance des consommateurs, le respect de la vie privée, la prévention des atteintes à la sécurité dans un contexte sociétal et la conformité aux réglementations sont autant de facteurs qui soulignent l'importance de cette responsabilité.

Ainsi, en examinant de près l'interconnexion entre l'encadrement juridique dans la protection des données personnelles et la responsabilité des entreprises, nous pouvons mieux comprendre les défis et les opportunités auxquels sont confrontées les entreprises dans cet environnement numérique en constante évolution.

Au cours de notre sujet, nous mettant en question ses dites notions éclaircis respectivement dans deux parties complémentaires, en 1ere partie nous étalerons la nature du cadre juridique relative à la protection des données personnelles au Maroc pour passer à la notion de la responsabilisation des entreprises au cours de leurs transactions électroniques, et parallèlement face à leur devoir éthique de protection de la confidentialité des données personnelles.

Plan:

Introduction

- ✓ **Partie1 : Cadre Juridique de la Protection des Données Personnelles au Maroc**
  - **Chapitre1 : la protection des données à caractère personnel**
- La contextualisation de la Loi 08-09
- Les Droits de la personne concerné.
  - **Chapitre2 : les services de confiances pour les transactions électroniques**
- Contextualisation de la loi 43-20
- Les services de confiance :

- ✓ **Partie2 : Responsabilité Juridique des Entreprises face aux Risques liés à la Violation des Données Personnelles**
  - **Chapitre1 : Les risques liés à la violation de la protection des données personnelles**
- Identification des risques
- Sanctions et mesures préventifs
  - **Chapitre2 : Bonnes pratiques et mesures de conformité pour les entreprises**
- Les obligations liées à la confidentialité et la sécurité du traitement des données professionnelles
- Approches de gestion des risques liés à la protection des données personnelles

Partie1 : Cadre Juridique de la Protection des Données Personnelles au Maroc

Chapitre1 : la protection des données à caractère personnel

❖ La contextualisation de la Loi 08-09

Les données à caractère personnel occupent de nos jours une place importante quant à leur omniprésence dans les interactions numériques. Ceux-ci permettent d'identifier directement ou indirectement une personne physique, Qu'il s'agisse de naviguer sur Internet, d'effectuer des transactions électroniques, d'utiliser une plateforme digitale ou des réseaux sociaux et même d'accéder à des services administratifs, les données personnelles sont constamment collectées, traitées et échangées.

De telle manière que cela pose de nombreux défis en matière de protection de la vie privée et de sécurité des informations. Ainsi Les risques de violation de la vie privée, de fraudes et d'abus nécessitent une vigilance accrue et des mesures de protection robustes.

C'est dans ce contexte que l'encadrement juridique des données à caractère personnel prend toute son importance. Des législations, telles que la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Sont essentielles pour établir des normes de protection élevées. Elles définissent les droits des individus, les obligations des responsables de traitement, et les conditions de traitement des données. En garantissant la sécurité, la confidentialité et l'intégrité des données personnelles, ces cadres juridiques permettent de renforcer la confiance des utilisateurs dans l'univers numérique et d'assurer un usage éthique et responsable des technologies de l'information.

Ainsi pour mieux comprendre ladite législation nous commençons tout d'abord par la définition de données à caractère personnel qui se présente comme :

« toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale»[1].

En outre, la législation numérique marocaine fut principalement inspirée de son homologue français, qui à son tour accorde une grande importance au droit numérique dans sa mission de réglementation du domaine du digital, le législateur français définit ainsi l'identité numérique et le recours à des moyens

[1] Dahir n 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

d'identification qui sont des données à caractère personnel au sens de la loi « Informatique et Libertés » qui définit les données à caractère personnel dans son article 2. Selon lequel :

Les Donnée à caractère personnel reflète : des informations se rapportant à une personne vivante identifiée ou identifiable. Différentes informations, dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel.

Des données à caractère personnel qui ont été rendues anonymes, chiffrées ou pseudonymisées, mais qui peuvent être utilisées pour identifier à nouveau une personne constituent toujours des données à caractère personnel et qui sont couvertes par le RGPD[2]

Dans ce volet, nous soulignons la similitude entre la définition des données à caractère personnel dans la législation marocaine et celle du RGPD de l'Union européenne, expliquée par plusieurs facteurs. Tout d'abord, l'intérêt du pays à adopter des normes internationales, étant donnée la large diffusion du RGPD comme référence mondiale en matière de protection des données personnelles. Et qui se traduit par le nombre important de pays, même en dehors de l'Union européenne, qui reconnaissent la pertinence et l'efficacité de ses principes et normes, amenant de telle sort, le Maroc à aligner sa législation sur ce règlement pour assurer une protection adéquate des données personnelles.

❖ Les Droits de la personne concerné.

- **Intégrité des informations numériques :**

L'intégrité numérique implique avant tout une reconnaissance de l'existence numérique des individus. Cela nécessite des droits spécifiques pour garantir à chacun la possibilité d'être protégé contre les préjudices, mais également d'être reconnu comme une personne libre, capable d'exercer son autonomie. Le droit à la protection de l'intégrité numérique est le corollaire de la capacité de l'individu à pouvoir s'engager dans un contrat, de voter ou tout simplement de prendre des décisions qui l'engagent dans une dimension numérique[3].

Ce droit repose également sur le consentement éclairé et explicite de la personne concernée, un principe fondamental qui fut souligné au niveau de l'article 4 de la loi 09-08, qui stipule que : « Le traitement des données, à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement à l'opération ou à l'ensemble des opérations envisagées.

2 À quoi correspondent les données à caractère personnel?

https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data

3 Notre si précieuse intégrité numérique : Plaidoyer pour une révolution hunamiste-Roussel,Alexis,Barbey,Grégoire, Slatkine Editions, 2021

Les données à caractère personnel objet du traitement ne peuvent être communiquées à un tiers que pour la réalisation de fins, directement liées aux fonctions du cédant et du cessionnaire et sous réserve du consentement préalable, de la personne concernée »[4]

L'idée que les données personnelles sont une partie essentielle de l'identité numérique d'un citoyen, et que celui-ci doit avoir le contrôle sur celles-ci comme il contrôle son intégrité physique, a été largement développée par plusieurs experts et penseurs dans le domaine de la protection des données et des droits numériques. Une des figures clés qui ont fortement contribué à cette réflexion est Laurence Devillers[5], une chercheuse française en intelligence artificielle et éthique, laquelle dans ses travaux soutient que les données personnelles doivent être considérées comme une extension de l'individu et qu'elles méritent une protection rigoureuse, tout comme l'intégrité physique d'une personne.

il existe également des experts marocains qui ont discuté de la protection des données personnelles et de l'identité numérique des citoyens. L'un des leurs est Driss Guerraoui, un économiste et professeur universitaire marocain. Qui a abordé les questions liées à la transformation numérique et à la protection des données personnelles dans le contexte marocain et africain. Tout en insistant sur l'importance pour les citoyens d'avoir le contrôle sur leurs données personnelles, tout comme ils maîtrisent leur intégrité physique, pour préserver leur dignité et leur liberté dans le monde numérique.

- **Droit à l'information :**

Le besoin d'informer les personnes concernées par une collecte de données est essentiel pour garantir la transparence et le respect de leurs droits. Le responsable en charge du traitement des données[6] est tenu de leur communiquer de manière claire et compréhensible la démarche entreprise ainsi que les droits dont elles peuvent bénéficier dans le cadre de cette collecte.

Cette communication peut prendre différentes formes, selon les circonstances et les préférences des personnes concernées. Par exemple, les précisions

[4] Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[5] Laurence Devillers est professeure à l'université Paris-Sorbonne et chercheuse au CNRS-LIMSI, où elle travaille sur les interactions homme-machine, la robotique sociale et l'éthique des technologies. Elle a écrit et parlé abondamment sur la nécessité de protéger les données personnelles des citoyens à une époque où l'intelligence artificielle et les grandes bases de données jouent un rôle central dans la société.

[6] Article1 de la loi 09-08 : « Le responsable du traitement est toute personne physique/ morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires, le responsable du traitement doit être indiqué dans la loi d'organisation et de fonctionnement ou dans le statut de l'entité légalement ou statutairement compétente pour traiter les données à caractère personnel en cause » ;

nécessaires peuvent être fournies via un site web, où une politique de protection des données à caractère personnel est mise à disposition. Cette politique devrait expliquer de manière détaillée les finalités de la collecte des données, les types de données collectées, les destinataires des données, ainsi que les droits des individus en matière de protection des données, tels que le droit d'accès, de rectification et d'opposition.

De même, les informations nécessaires peuvent être intégrées dans des clauses contractuelles, notamment lorsqu'il s'agit de relations commerciales ou contractuelles entre le responsable du traitement et les personnes concernées. Ces clauses contractuelles devraient clairement indiquer la manière dont les données seront utilisées, traitées et protégées, ainsi que les droits dont les individus disposent en vertu de la législation sur la protection des données.

En fournissant ces informations de manière proactive et transparente, le responsable du traitement des données renforce la confiance des individus dans le traitement de leurs données personnelles. Qui permet également aux personnes concernées de prendre des décisions éclairées sur la manière dont leurs données sont utilisées et traitées, tout en leur donnant les moyens d'exercer leurs droits en matière de protection des données.

L'article 5 de la loi 09-08 développe d'avantage la signification du droit à l'information lors de la collecte des données, par laquelle il invoque toute personne sollicitée directement, en vue d'une collecte de ses données personnelles, toute personne qui doit être préalablement informé de manière expresse, précise et non équivoque par le responsable de traitement ou son représentant, sauf si elle en a déjà eu connaissance des éléments suivants ;

Chapitre2 : les services de confiances pour les transactions électroniques

❖ Contextualisation de la loi 43-20 :

Les principes du droit des contrats sont anciens : ils ont été formés dans un monde basé sur le papier et l'encre. Ainsi, la rencontre des esprits dans le cyberespace n'a jamais été envisagée, et la validité et l'effet de l'utilisation de messages électroniques dans les communications commerciales n'ont jamais été envisagés. Des exigences telles que l'écriture et la signature ne peuvent pas être traduites dans le monde virtuel du commerce électronique sans intervention législative. D'autres problèmes courants de l'e-contrat comprennent : la valeur juridique et la validité des communications électroniques ; le respect des formalités ; la détermination du moment et du lieu de conclusion d'un contrat ; et la validité des transactions automatisées. Un problème juridique découlant de l'utilisation des communications électroniques est l'admissibilité et le poids probant de la preuve électronique. Le temps et le lieu conventionnels ont été

remplacés par "à tout moment, n'importe où", dans un monde interconnecté[7]. Ainsi fut la perception de la transition numérique du monde occidental.

En outre, la validité et l'applicabilité des transactions électroniques ont fait l'objet d'efforts législatifs mondiaux considérables. Le gouvernement fédéral des États-Unis, les 50 États américains, l'Union européenne et la plupart des gouvernements des pays ont promulgué une forme de législation régissant cette fameuse digitalisation[8].

C'est dans cette perspective que rejoint le Maroc les pas des géants de l'industrie mondial et traça sa propre stratégie d'ouverture sur le processus de transformation digitale, inspiré et orienté par des initiatives gouvernementales nationale telles que la stratégie Maroc Digital 2020[9]. Ainsi, la digitalisation commence à occuper une place de plus en plus centrale dans le développement économique et social du royaume, jouant un rôle clé dans la modernisation des infrastructures et des services. Et il en va de même que, l'essor de la certification électronique et des transactions électroniques s'inscrit dans cette dynamique, qui vise à renforcer la sécurité, l'efficacité et la transparence des échanges commerciaux et administratifs.

En effet, la certification électronique devint une composante essentielle de processus de la digitalisation, particulièrement en ce qui concerne les transactions électroniques, mettant en question l'intégrité et la confidentialité des échanges.

En effet et étant donné l'important développement au niveau du sujet de la certification électronique et des transactions électroniques au Maroc, associé à l'opportunité majeure qui s'offre au pays s'inscrire dans l'économie numérique mondiale.

Des cadres réglementaires appropriés se sont établie de telle manière que cela favorisera l'épanouissement des transactions électroniques et augmentera la confiance des acteurs économiques vis-à-vis des services de confiances et des mécanismes de signature électronique.

Nous soulignons, dans ce contexte, la loi 53-05 relative à l'échange électronique de données juridiques, comme premier texte dans cette perspective des transactions électronique, un effort important du législateur marocain mais qui manqua cependant de fondement et se caractérisa avec de la rigidité, ce qui s'est traduit avec la grande avancé de lere digital, par la nécessité d'actualiser, de clarifier, d'harmoniser et d'améliorer la réglementation des transactions

[7] Establishment of Harmonized Policies for the ICT Market in the ACP DRAFT Southern African Development Community (SADC) MODEL LAW ON ELECTRONIC TRANSACTIONS AND ELECTRONIC COMMERCE, page 3

[8] The Legal Challenges of Implementing Electronic Transactions, Thomas J Smedinghoff, page 6

[9] Une stratégie visant à intégrer davantage les technologies de l'information et de la communication (TIC) dans les secteurs public et privé, afin de stimuler l'innovation, la compétitivité et la croissance économique

électroniques pourvu de répondre aux besoins actuels et aux normes internationales.

Ladite vision inspira par la suite l'élaboration du texte actualisé encadrant les transactions électroniques au Maroc à savoir la loi 43-20 relative aux services de confiance pour les transactions électroniques, ce qui aborde la question de l'ensemble des échanges, correspondances, contrat, acte et toute autre transaction conclue ou exécutée, en tout ou en partie, par voie électronique, selon son article 2 ;

❖ Les services de confiance :

Les services de confiance jouent un rôle crucial dans les transactions électroniques en assurant la sécurité, l'intégrité et l'authenticité des échanges numériques. Selon l'article 3 de la loi 43-20 Ils englobent divers mécanismes tels que la signature électronique, les certificats numériques, les horodatages et la gestion des identités numériques10, tous conçus pour renforcer la confiance des utilisateurs dans le monde numérique. Ces services permettent de garantir que les informations échangées sont fiables et vérifiées, offrant ainsi une base solide pour le développement de l'économie numérique.

En effet les services de confiance jouent un rôle fondamental dans les transactions électroniques en garantissant la sécurité, l'intégrité et l'authenticité des échanges numériques. Ces services comprennent le traitement numérique des transactions. Ils constituent une base essentielle pour instaurer la confiance dans les interactions en ligne, assurant ainsi que les informations échangées sont fiables et vérifiées.

Dans ce cadre, la promulgation de la loi 43-20 a été un pas décisif pour lever les obstacles juridiques entravant le développement de ces services de confiance. Ladite législation a introduit des modifications cruciales, notamment l'ajout de différents niveaux de signatures électroniques pour mieux encadrer les transactions numériques. Marqué principalement par son inspiration de la réglementation européenne par laquelle elle implémente un niveau intermédiaire de signature électronique dit « avancé », en plus des niveaux « simple » et « qualifié » à la législation antérieur (la loi 53-0511)

1. Le premier niveau, **la signature électronique « simple »,** qu'est conçu pour un usage simplifié sans exigences techniques ou fonctionnelles spécifiques. Il a été définit par l'article 2 de la loi 43-20 par référence à l'usage de procédés

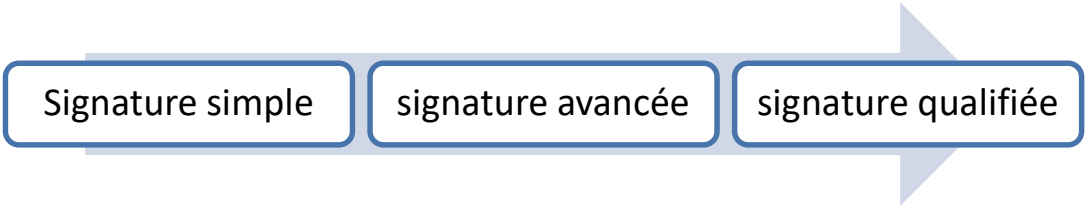
[10] Dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020) portant promulgation de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques : article 03

[11] Dahir n 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi 53-05 relative à l'échange électronique de données juridiques

fiables d'identification électronique, exprimant le consentement du signataire ; une simplicité dans le processus, confrontée toutefois, à un niveau de sécurité faible[12], ce qui signifie que la charge de la preuve de l'authenticité de la signature repose sur le défendeur en cas de litige.

2. Le deuxième niveau, **la signature électronique « avancée »**, qui offre une meilleure reconnaissance juridique que le niveau simple et impose des exigences techniques et organisationnelles intermédiaires, elle est introduite selon l'article 5 de la loi 43-20, comme une méthode de signature électronique qui présente des caractéristiques spécifiques pour garantir son intégrité et son authenticité. En effet, ce type de signatures doit être unique à son signataire, permettant ainsi une identification claire de ce dernier. De plus, la signature électronique avancée est créée à partir de données de signature électronique sous le contrôle exclusif du signataire, assurant ainsi un niveau élevé de confiance.

3. Enfin, le niveau « **qualifié** » représente le plus haut degré de sécurité et de fiabilité. Il requiert l'utilisation obligatoire de produits de cryptographie et bénéficie de la présomption de fiabilité, ce qui signifie que l'authenticité de la signature est présumée jusqu'à preuve du contraire. Il a été défini au niveau de l'article 6 de la loi 43-20 par référence au dispositif qualifié de création de signature électronique qui atteste la conformité de la signature par un certificat de conformité[13] délivré par l'autorité nationale.



En instituant ces trois niveaux de signatures électroniques, la loi 43-20 permet d'adapter les exigences de sécurité et de fiabilité aux différents types de transactions électroniques, facilitant ainsi leur adoption à grande échelle.

Partie2 : Responsabilité Juridique des Entreprises face aux Risques liés à la Violation des Données Personnelles

Chapitre1 : Les risques liés à la violation de la protection des données personnelles

❖ <u>Identification des risques</u>

- **Risque juridique pour le responsable du traitement**

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement des données personnelles ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles

[12] Guide de sélection du niveau des signatures et des cachets électroniques, page 09

[13] Article 8 de la loi 43-20, relative aux services de confiance pour les transactions électroniques.

appropriées pour s'assurer et être en mesure de démontrer que le traitement des données personnelles est effectué conformément aux dispositions des lois relatifs au traitement des données personnelles[14],

1. Droit d'information face au risque de l'opacité :

D'après l'article 5 de la loi 09-08, concernant la collecte de données sur les réseaux ouverts, le rôle du responsable de traitement des données s'avère manifestement crucial pour garantir la transparence et la sécurité des informations personnelles. Lors de cette étape, le responsable de traitement a l'obligation d'informer la personne concernée des risques spécifiques associés à la circulation de ses données sur les réseaux ouverts. Cette obligation d'information comprend la clarification que les données à caractère personnel peuvent être transmises sans garanties de sécurité adéquates et qu'elles risquent d'être lues et utilisées par des tiers non autorisés.

Le responsable de traitement doit donc s'assurer que la personne concernée est pleinement consciente de ces risques avant de consentir à la collecte de ses données.

Cette étape implique la responsabilité du responsable de traitement, dans son premier contact avec les données personnelles.

2. Droit d'accès face au manque de communication

L'existence d'un droit d'accès aux données à caractère personnel conformément à l'article 7 de la loi 09-08 et du droit de rectification de ces données[15], tous deux sont fondamentales dans le cadre de la protection de la vie privée et des droits individuels. Ce droit permet à une personne de savoir quelles informations sont détenues à son sujet et de les corriger si elles sont inexactes ou incomplètes. Cela revêt une importance particulière dans les situations où les données sont collectées, car il représente une garantit d'un traitement équitable des données à l'égard de la personne concernée.

Encore une fois, la responsabilité du responsable de traitement est engagée étant l'intermédiaire entre les données traitées et la personne concerné par ce

[14] Le règlement général sur la protection des données-RGPD/Chapitre IV- responsable du traitement et sous-traitant, https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article24

[15] Article 8 de la loi 09-08 : « La personne concernée, justifiant de son identité, a le droit d'obtenir du responsable du traitement : L'actualisation, la rectification, l'effacement ou le verrouillage des données à caractère personnel dont le traitement n'est pas conforme à la présente loi, notamment en raison du caractère incomplet et inexact de ces données ; le responsable du traitement est tenu de procéder aux rectifications nécessaires sans frais pour le demandeur et ce, dans un délai franc de dix jours… ».

traitement, dans le contexte de ce que le législateur définit par le droit d'accès et de rectification aux données personnelles collectés

Concrètement, cela signifie que le responsable de traitement doit mettre en place des procédures permettant aux individus d'exercer leurs droits, telles que la mise en place d'un processus clair et transparent pour faire une demande d'accès ou de rectification des données.

- **Risque juridique pour le délinquant informatique**

Parallèlement à l'expansion remarquable des outils numériques dans la société marocaine, tant au sein des entreprises commerciales que dans d'autres domaines, cette avancée a été accompagnée par une série d'enjeux touchant à la fois les opportunités offertes par les mécanismes numériques et les risques associés à la cybercriminalité. La cybercriminalité représente en effet une menace croissante pour les individus, les entreprises et les gouvernements du monde entier. Les avancées technologiques, bien qu'elles offrent des opportunités sans précédent pour le développement économique et social, ont également ouvert la porte à de nouvelles formes de criminalité. Les attaques informatiques, qu'il s'agisse de piratage, de vol de données, de ransomwares ou de fraude en ligne, des actes qui peuvent avoir des conséquences dévastatrices, en compromettant la confidentialité des informations, la sécurité des infrastructures critiques et la confiance dans les systèmes numériques des entreprises dans le cas d'exemple de la cyberattaque subie par la société de renom Dell, l'un des plus grands fabricants de PC au monde, à laquelle en avril 2024 un hacker coupable de délinquance informatique vola les données personnelles de 49 millions de clients[16] de l'entreprise, dans une tentation de trafique desdites informations confidentielles à des tiers.

Dans ce contexte, la protection des données personnelles est devenue alors un enjeu majeur. Face à ces défis, La loi 07-03 instaura au Maroc un cadre juridique orienté vers la répression des crimes informatiques, en abordant le sujet des infractions informatiques telles que :

- **L'accès frauduleux aux systèmes informatiques**[17],

Définit Selon l'article 4(12) du RGPD[18], entant que toute violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte,

[16] Dell victime d'une cyberattaque : 49 millions de données des clients volées, https://cybersecuritymag.africa/index.php/dell-victime-de-cyberattaque-49-millions-de-donnees-des-clients-volees

[17] dans le cas d'exemple de Dell susmentionné

[18] 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)

l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. Au niveau national l'article 607-3 de la loi marocain 07-03 s'oriente directement vers la répression et dans ce cas d'espèce, le législateur prévois une peine d'emprisonnement d'un mois à trois mois et de 2 000 à 10 000 dirhams d'amende ou de l'une de ces deux peines[19].

- **L'entrave au fonctionnement des systèmes informatiques, l'introduction illicite de données et l'utilisation de dispositifs malveillants,**

Des infractions qui peut être définie comme toute action délibérée visant à perturber, ralentir ou empêcher le bon fonctionnement d'un système informatique. Selon l'Article 607-5 du Code pénal marocain, les infractions furent interprétées par le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé de données, auxquels le législateur prévoie une peine d'emprisonnement d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende, ou de l'une de ces deux peines seulement.

❖ Sanctions et mesures préventifs

L'inclusion des sanctions, au niveau de la législation sur la sécurité informatique revêt une importance capitale, à la fois, pour la protection des données personnelles et à la responsabilisation des entreprises chargées du traitement de ces données.

En effet ces mesures de protection et de répression jouent un rôle important dans le cadre de la lutte du législateur marocain contre les violations de la confidentialité des données. En établissant un arsenal de conséquences y correspondants et des sanctions qui encourageront les entreprises à prendre au sérieux leur responsabilité en matière de protection des données.

Dans ce contexte nous citerons on ce qui suit les grandes lignes de ces mesures répressives :

- **Le manquement aux obligations de déclaration et d'autorisation avant l'utilisation des données personnelles :**

Tels manquements sont sévèrement punis par la législation marocaine. En référence à l'article 52 de la loi 09-08 qui souligne l'importance de l'étape de la déclaration et de l'obtention de l'autorisation du traitement des données depuis la commission nationale de contrôle de la protection des données à caractère personnel.

Le législateur explique que l'utilisation d'un fichier de données personnelles sans avoir effectué la déclaration ou obtenu l'autorisation requise conformément à l'article 12, peut être traduit par une amende de 10 000 à 100 000 DH.

[19] Dahir n°1-03-197 du 16 ramadan 1424 (11 novembre 2003) portant promulgation de la loi n°07-03 complètent le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé de données.

En outre, au niveau de l'article 57 le législateur met en avant l'importance du consentement pourvu de crédibiliser le processus de traitement des données personnelles, dans ce contexte le consentement, inclut l'ensemble des données révélant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, ainsi que les données relatives à la santé. De telles infractions peuvent entraîner la personne coupable d'une peine d'emprisonnement de six mois à deux ans et d'une amende allant de 50 000 à 300 000 DH, ou l'une de ces deux peines seulement.

- **Le refus des droits des personnes concernées sur leurs données personnelles**

Dans ce cadre, L'article 53 de la loi 09-08 énonce que toute personne responsable du traitement des données personnelles et qui refuse les droits d'accès, de rectification ou d'opposition est passible d'une amende allant de 20.000 à 200.000 DH par infraction.

- **Collecte Frauduleuse et Illicite de Données Personnelles**

Quiconque collecte des données personnelles de manière frauduleuse, déloyale ou illicite, ou les utilise pour des finalités non déclarées ou non autorisées, peut être condamné à une peine d'emprisonnement allant de trois mois à un an. Une amende variant de 20 000 à 200 000 dirhams peut également être imposée, ou l'une de ces deux peines seulement[20].

Les mêmes sanctions s'appliquent à toute personne qui conserve des données personnelles au-delà de la durée autorisée par la loi en vigueur ou celle spécifiée dans la déclaration ou l'autorisation.[21]

Les articles 58, 59 et 60 établissent les sanctions en cas de non-respect de la loi concernant le traitement des données personnelles. Selon l'article 58, toute personne qui effectue un traitement de données personnelles sans respecter la loi est passible d'une peine d'emprisonnement de trois mois à un an et d'une amende de 20 000 à 200 000 DH, ou de l'une de ces deux peines seulement.

- **Les sanctions pour les responsables de traitement**

Dans ce cas d'espèce le législateur étale les lignes de la responsabilité du responsable de traitement d'une entreprise qui en raison de ses fonctions, facilite ou cause par négligence un usage abusif ou frauduleux des données personnelles traitées ou reçues par les services de l'entreprise, ou qui divulguent des informations confidentielles à des tiers non autorisés. Ainsi pour remédier à ses situations le législateur prévoie une peine d'emprisonnement de six mois à un an

[20] Article 54 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

[21] Article 55 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

et une amende de 20 000 à 300 000 DH, ou l'une de ces deux peines. Dans une vision non seulement de répression mais aussi de dissuasion en amont et qui envoie un message fort aux responsables de traitement et aux entreprises sur l'importance cruciale de la protection des données personnelles.

Chapitre2 : Bonnes pratiques et mesures de conformité pour les entreprises

❖ Les obligations liées à la confidentialité et la sécurité du traitement des données professionnelles

L'utilisation des nouvelles technologies de l'information constitue de toute évidence un outil compétitif fondamental pour les entreprises. Dès lors, il existe un marché des données personnelles lesquelles se monnaient entre les différents acteurs de la vie économique. Cette mutation du mode de fonctionnement de l'entreprise « la rend plus performante, mais aussi plus vulnérable, ce qui l'oblige à repenser sa politique de sécurité »[22] .

Les risques pesant sur les entreprises en la matière sont nombreux. Failles de sécurité, fuite de l'information, vol et divulgation de données sensibles, fraudes externes ou internes aux systèmes d'information, piratage ou encore espionnage, autant d'éléments pouvant engager la responsabilité administrative, civile et pénale des entreprises, outre le risque lié à sa réputation que représente tout manquement à la sécurité des données des personnes physiques (salariés, clients, consommateurs, prospects, partenaires, etc.)

Les entreprises présentent de ce fait, un rôle ambigu, à la fois victimes potentielles de cyber attaques et responsables de la sécurité des données personnelles y traitées. Ceci leur impose de mettre en œuvre une politique de gestion des risques tant internes qu'externes en matière de données personnelles, conciliant cette exigence sécuritaire aux intérêts légitimes de l'entreprise et aux droits fondamentaux de protection des données personnelles et de respect de la vie privée.

En effet, la confidentialité et la sécurité des données professionnelles revêtent une importance capitale dans le cadre de la protection des informations personnelles. Que ce soit de manière générale ou dans un contexte professionnel, pour les entreprises, ainsi, la protection des données personnelles, impose que les employeurs informent clairement leurs employés sur la nature des données collectées et les raisons de cette collecte. Les responsables de traitement doivent également informer les personnes concernées sur plusieurs points essentiels, tels que l'identité du responsable de traitement, les finalités du traitement, les destinataires des données, et les droits des individus concernant leurs données

[22] P. ACHILLEAS, J.-Cl. Libertés, Fasc. 820 : Internet et libertés

(accès, rectification, opposition). Cette transparence est cruciale pour instaurer un climat de confiance entre les employeurs et les employés, et pour garantir le respect des droits fondamentaux des individus.

De plus, la loi 09-08 stipule que les données personnelles ne doivent pas être conservées par l'entreprise au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Les employeurs doivent donc définir et respecter des délais de conservation appropriés. Par exemple, les données relatives à un ancien employé ne doivent pas être conservées indéfiniment, sauf s'il existe des obligations légales spécifiques justifiant une conservation prolongée.

Et en cas de violation de données personnelles, les responsables de traitement dans une entité ont l'obligation d'informer les personnes concernées ainsi que la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). Cette notification doit être effectuée dans les meilleurs délais afin de permettre aux personnes concernées de prendre les mesures nécessaires pour se protéger.

En effet, les employeurs, en tant que responsables de traitement, sont pleinement responsables de la protection des données personnelles de leurs employés[23]. Ils doivent s'assurer de la conformité de leurs pratiques avec la loi 09-08 et sensibiliser leur personnel à l'importance de la protection des données. La mise en place d'une politique de protection des données et la désignation d'un délégué à la protection des données peuvent constituer des mesures efficaces pour garantir cette conformité. Etant donné que la non-conformité aux dispositions de la loi 09-08 expose les responsables de traitement à des sanctions administratives et pénales. La CNDP est alors habilitée à infliger des amendes en cas de non-respect des obligations en matière de protection des données et des sanctions pénales peuvent être prononcées en cas d'infractions graves, telles que la collecte de données sans consentement ou la divulgation non autorisée de données.

❖ Approches de gestion des risques liés à la protection des données personnelles

Dans cette approche gestionnaire, le rôle de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) est essentiel. Dans le sens où cet organisme joue un rôle de supervision et de régulation pour garantir à ce que les entreprises respectent les dispositions légales en matière de protection des données. Ainsi, la surveillance, l'audit et la

[23] « L'entreprise marocaine constitue aujourd'hui un levier fondamental de l'effectivité de la politique de protection des données personnelles, rôle initialement imposé par les pouvoirs publics mais que l'entreprise a su s'approprier, en intégrant progressivement l'impératif de protection des données personnelles à la culture d'entreprise jusqu'à en faire une arme concurrentielle » Lagtati Kamal. "La protection des données personnelles en entreprise au Maroc". Signatures internationales, 2022, n° 6, page 170

sensibilisation deviennent des leviers stratégiques pour assurer la conformité et la sécurité des données personnelles.

Ladite surveillance, permet de vérifier le respect des normes et règlements en vigueur par les entreprises, par le biais d'inspections régulières et des enquêtes ciblées, lesquelles garantissent que les entreprises collectent, traitent et stockent les données personnelles de manière sécurisée et conforme à la loi. Une surveillance qui contribue à dissuader les pratiques non conformes et à encourager les entreprises à adopter des politiques de protection des données rigoureuses.

Par ailleurs, l'audit joue également un rôle crucial dans l'évaluation de l'efficacité des mesures de sécurité mises en place par les entreprises. La CNDP peut réaliser des audits de conformité pour évaluer la gestion des risques liés à la protection des données personnelles au sein des entreprises. Enfin, la sensibilisation constitue un volet essentiel pour la propagation d'une culture de la protection des données au sein des entreprises. Ainsi la CNDP organise des campagnes de sensibilisation et des formations destinées aux dirigeants, aux employés et aux responsables de traitement pour les informer sur les enjeux de la protection des données et sur les bonnes pratiques à adopter. De telle sort qu'en sensibilisant les acteurs concernés, la CNDP contribue à renforcer les compétences et les connaissances nécessaires pour assurer une gestion responsable et sécurisée des données personnelles.

Bibliographie :

- **Documentation:**

- L'identité numérique dans le droit et la pratique, Éric A Caprioli, Isabelle Cantero,Ilène Choukri, Pascal Agosti, RB Éditions, Dans la collection Droit, 2017
- Notre si précieuse intégrité numérique : Plaidoyer pour une révolution hunamiste- Roussel,Alexis,Barbey,Grégoire, Slatkine Editions, 2021
- Establishment of Harmonized Policies for the ICT Market in the ACP DRAFT Southern African Development Community (SADC) Model Law on electronic transactions and electronic commerce
- The Legal Challenges of Implementing Electronic Transactions, Thomas J Smedinghoff
- Guide de sélection du niveau des signatures et des cachets électroniques
- 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)

- **Lois:**

- Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la **loi n° 09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- Dahir n°1-03-197 du 16 ramadan 1424 (11 novembre 2003) portant promulgation de la **loi n°07-03** complètent le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé de données.
- Dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020) portant promulgation de la **loi n° 43-20** relative aux services de confiance pour les transactions électroniques
- Dahir n 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la **loi n°53-05** relative à l'échange électronique de données juridiques

- **Articles:**

- La valeur juridique de l'écrit électronique en droit Marocain et comparé, Hamza Jabir, Ali Ou-Yacoub, Revue Internationale du chercheur, 2022
- À quoi correspondent les données à caractère personnel,https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data
- Le règlement général sur la protection des données-RGPD/Chapitre IV-responsable du traitement et sous-traitant, https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article24
- La protection des données personnelles en entreprise au Maroc". Lagtati Kamal. Signatures internationales, 2022, n° 6