



LES DONNÉES PERSONNELLES À L’ÈRE DU BIG-DATA : QUEL CADRE JURIDIQUE AU MAROC ?

PERSONAL DATA IN THE AREA OF BIG-DATA: WHAT LEGAL FRAMEWORK IN MOROCCO?

HAOUNANI AMINE

Doctorant en droit du numérique et des nouvelles technologies

Faculté des Sciences Juridiques et Politiques- Settat

Université Hassan Premier

Laboratoire De Recherche En Dynamiques Sécuritaires

Maroc

A.haounani@uhp.ac.ma

AKKOUR SOUMAYA

Professeure d’enseignement supérieur

Faculté des Sciences Juridiques et Politiques- Settat

Université Hassan Premier

Laboratoire De Recherche En Dynamiques Sécuritaires

Maroc

Soumiasta@yahoo.fr

Date de soumission : 12/02/2023

Date d’acceptation : 05/03/2023

Pour citer cet article :

HAOUNANI. A, & AKKOUR. S. (2023), « LES DONNEES PERSONNELLES A L’ERE DU BIG-DATA : QUEL CADRE JURIDIQUE AU MAROC ? », Revue Internationale du chercheur « Volume 4 : Numéro 1» pp : 429- 446

Résumé

Au Maroc, la protection des données personnelles est réglementée par la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, adoptée en 2009. Cette loi définit les principes fondamentaux pour le traitement des données personnelles, tels que le respect de la vie privée, la transparence, la responsabilité et la sécurité des données. Dans l'ère du Big Data, où de vastes quantités de données sont collectées, stockées et utilisées pour diverses fins, il est important que les entreprises et les gouvernements respectent les droits des citoyens en matière de protection de leurs données personnelles. La loi marocaine sur la protection des données personnelles s'applique aux entreprises nationales et étrangères opérant au Maroc qui collectent, stockent ou traitent des données personnelles de citoyens marocains.

Dans cet article, nous allons présenter et analyser la protection des données personnelles à l'ère du Big Data, en analysant le cadre juridique et institutionnel assurant cette protection, dans le but de déterminer si la législation marocaine sur la protection des données à caractère personnel est suffisamment efficace pour garantir la protection des données personnelles dans un contexte de Big Data.

Mots clés : « Les données personnelles » ; « Vie privée » ; « La protection » ; « Le traitement » ; « Big data ».

Abstract

In Morocco, the protection of personal data is regulated by Law 09-08 concerning the protection of individuals with regard to the processing of personal data, adopted in 2009. This law defines the fundamental principles for the processing of personal data, such as respect for privacy, transparency, accountability, and data security.

In the era of Big Data, where vast amounts of data are collected, stored, and used for various purposes, it is important that businesses and governments respect citizens' rights in protecting their personal data. The Moroccan law on the protection of personal data applies to national and foreign companies operating in Morocco that collect, store, or process personal data of Moroccan citizens.

In this article, we will present and analyze the protection of personal data in the era of Big Data, by examining the legal and institutional framework ensuring this protection, with the aim of determining whether Moroccan legislation on the protection of personal data is sufficiently effective to guarantee the protection of personal data in a Big Data context.

Keywords: « Personal data »; « Privacy »; « Protection »; « Processing »; « Big data ».

Introduction

Depuis le début des années 2000, le Royaume a mis en place des réformes pour trouver un équilibre entre la sécurité et la protection de la vie privée. Ces réformes visent à garantir la protection des données personnelles et des données massives. La protection de la vie privée est un enjeu clé pour le Royaume et les réformes en cours tendent à renforcer les garanties pour les citoyens. Les réformes sur la protection de la vie privée sont en constante évolution pour s'adapter aux nouvelles technologies et aux nouveaux enjeux de sécurité. Les données massives sont particulièrement importantes dans cette réforme, car elles ont un impact considérable sur la vie privée des citoyens. C'est un chantier en plein essor qui a pour but de protéger les données personnelles des citoyens tout en garantissant la sécurité du pays.

Grace à la réforme constitutionnelle de juillet 2011, Le Maroc a pris position pour renforcer la protection des citoyens contre l'utilisation abusive de traitement automatisé des données personnelles et il a renforcé son arsenal juridique et institutionnel à travers plusieurs lois et institutions, notamment la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que la commission nationale de contrôle de la protection des données à caractère personnelles qui est l'institution nationale pour assurer la protection des données à caractère personnel et des données massives au Maroc.

Le Big Data désigne la grande quantité de données produites par les activités humaines, principalement en ligne, et l'utilisation de ces données pour obtenir des insights et prendre des décisions. Les données personnelles font partie intégrante de Big Data, car elles représentent une source importante de données et peuvent être utilisées pour l'analyse de grandes quantités de données. Cependant, il y a des préoccupations concernant la protection des données personnelles en relation avec Big Data, car l'analyse de données massives peut révéler des informations très personnelles sur les individus, menaçant ainsi leur vie privée. Il est donc crucial de mettre en place des réglementations et des mesures de sécurité pour garantir que les données personnelles sont utilisées de manière responsable et respectueuse de la vie privée des individus.

D'autre part l'évolution massive des volumes de données et l'intensification de l'exploitation de ses données par les entreprises ont transformé radicalement l'économie numérique. Cette transformation n'a pas été sans modifier préalablement les relations que les utilisateurs entretiennent avec leurs données personnelles. Plus profondément c'est l'image de la vie privée qui semble avoir été bouleversée.



L'intérêt de notre sujet s'incline par les efforts du législateur Marocain afin de favoriser l'efficacité et l'efficience de l'arsenal juridique assurant la protection des données à caractère personnel et le cadre juridique des données massives.

La problématique sous-jacente concerne l'efficacité de la législation marocaine relative à la protection des données personnelles, spécifiquement dans le cadre du Big Data, en vue d'assurer une protection adéquate de ces données sensibles, ce qui nous penche à poser la question suivante :

- ❖ Comment assurer une protection adéquate des données personnelles dans le contexte du Big Data au Maroc en évaluant les lacunes de la législation actuelle et en proposant des mesures renforçant la protection de ces données sensibles ?

Pour aborder cette problématique, nous allons utiliser une méthodologie analytique qui consistera à examiner la distinction entre les données personnelles et les données massives, ainsi que le cadre juridique et institutionnel relatif à la protection des données personnelles et des données massives au Maroc.

Partant de ce constat, il serait légitime alors de s'interroger sur la distinction entre les données personnelles et Big-data pour mieux savoir la distinction entre ces deux notions (1).

En second lieu nous traiterons l'arsenal juridique et institutionnel assurant la protection des deux notions, avec une analyse approfondie de la loi 09-08¹ (2).

1. Les données personnelles entant qu'un noyau du Big- data :

Le Big Data utilise les données personnelles en grande quantité pour des analyses précises, mais leur utilisation pose des problèmes de confidentialité et de protection de la vie privée, nécessitant des politiques claires de confidentialité.

1.1 Le cadre définitionnel des données personnelles et du Big-data :

La protection des données personnelles est une préoccupation majeure dans l'utilisation du Big Data. Il est donc important de définir clairement les termes utilisés, notamment les données personnelles et le Big Data.

¹ La loi 09-08¹ relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.



1.1.1 Le cadre définitionnel des données personnelles :

D'un point de vue économique, les données personnelles sont des informations qui ont une valeur économique pour les entreprises et les organisations. Elles sont considérées comme un actif commercial important, car elles peuvent aider les entreprises à mieux comprendre les besoins et les préférences des consommateurs, ainsi qu'à prendre des décisions commerciales plus éclairées.

Les données personnelles peuvent être de plusieurs types, tels que les informations d'identification, les données de localisation, les informations sur les achats et les préférences de consommation, les données de santé, les informations financières et autres informations personnelles sensibles.

Les entreprises peuvent utiliser ces données pour des activités commerciales telles que le marketing ciblé, la personnalisation des offres de produits et services, la recherche et le développement de nouveaux produits, l'analyse de données et la prise de décisions commerciales stratégiques.

Il est important de noter que la collecte et l'utilisation de données personnelles sont régies par des lois et réglementations spécifiques, telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne et la Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel au Maroc. Ces lois visent à protéger les droits et la vie privée des individus en contrôlant la collecte, le stockage, le traitement et le transfert de leurs données personnelles.

D'un point de vue juridique, les données personnelles sont des informations relatives à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Cela inclut les noms, les adresses, les numéros de téléphone, les adresses e-mail, les données bancaires, les informations de localisation, les photos, les vidéos, etc.

Le législateur Marocain a défini, dans son article premier de la loi 09-08, les données à caractère personnel comme étant : « toute information de quelque nature qu'elle soit et indépendamment



de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable »².

Les personnes concernées sont celles qui sont identifiées ou qui peuvent être identifiées directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de leur identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

1.1.2 La notion du big-data :

Les données massives désigne l'ensemble des données et informations générées par les activités humaines, surtout sur internet. Ces données peuvent être structurées comme celles contenues dans une base de données ou non structurées comme les données textuelles ou géospatiales. Le big data se caractérise par sa grande quantité, sa diversité et sa vitesse de génération, ce qui rend difficile son traitement et son analyse avec les technologies et méthodologies traditionnelles. On l'utilise souvent pour obtenir de meilleures insights et prendre de meilleures décisions dans la santé³, la finance, la publicité, la recherche, etc.

Pour traiter et analyser le big data, on utilise des outils de gestion de données, des technologies de stockage et de traitement en masse, ainsi que des algorithmes et modèles statistiques.⁴

Il existe plusieurs composants qui entrent en jeu dans le concept de "big data" :

- Les données : Le "big data" fait référence à de très grandes quantités de données, qui peuvent être structurées c'est-à-dire organisées de manière ordonnée, comme dans une base de données ou non structurées (c'est-à-dire non organisées de manière ordonnée, comme les données textuelles ou les données provenant de médias sociaux).
- Les technologies de l'information : Pour gérer et analyser les données du "big data", il est nécessaire d'utiliser des technologies de l'information spécialisées, telles que des bases de données distribuées, des outils d'analyse de données en temps réel, etc.

² L'article 1 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

³ Le règlement européen est entré en application le 25 mai 2018. Il définit les données à caractères personnelles concernant la santé comme regroupant à la fois les informations sur la santé, mais aussi des données de mesures non en lien avec de la pathologie et les données d'usagers du système de santé

⁴ HAOUNANI Amine - L'utilisation des données personnelles dans le droit comparé – mémoire pour l'obtention du Master Droit du Numérique 2019. P 77



- Les algorithmes d'analyse de données : Pour extraire des informations utiles des données du "big data", il est nécessaire d'utiliser des algorithmes d'analyse de données qui peuvent identifier des modèles, des tendances et des relations cachées dans les données.
- Les personnes : Le "big data" ne peut être exploité de manière efficace sans les compétences et les connaissances des personnes qui sont chargées de le gérer et de l'analyser. Cela peut inclure des data scientifiques, des ingénieurs de données, des analystes de données, etc.
- Les processus : Il est très important de mettre en place des processus efficaces pour collecter, stocker, gérer et analyser les données du "big data". Cela peut inclure des processus de gestion de la qualité des données, de sécurité des données, de gestion des droits d'accès aux données, etc.

1.2 Les données personnelles à l'ère des données massives

À l'ère des données massives, les données personnelles sont devenues un atout commercial crucial pour les entreprises, qui cherchent à mieux comprendre leurs clients et à optimiser leurs stratégies commerciales. Cependant, la collecte et l'utilisation de ces données ont suscité des préoccupations croissantes en matière de sécurité des données, de confidentialité et de surveillance.

1.2.1. Le rôle des données personnelles dans le big-data :

Les données personnelles sont un élément central du big data, car elles permettent de capturer des informations sur les individus et de les utiliser pour diverses fins. Les données personnelles peuvent inclure des informations telles que le nom, le prénom, le numéro de téléphone, l'adresse traditionnelle ou électronique, le numéro de téléphone, les préférences et les intérêts de chaque personne. Elles peuvent être collectées de différentes manières, par exemple lorsque vous remplissez un formulaire en ligne, utilisez un service en ligne ou naviguez sur le web⁵. Le big data est souvent utilisé pour obtenir des insights sur les comportements et les préférences des individus, ce qui peut être utile pour les entreprises et les organisations dans leur stratégie de marketing et de communication. Par exemple, en analysant les données personnelles, une entreprise peut mieux cibler ses campagnes publicitaires et offrir des produits et services personnalisés en fonction des intérêts et des besoins de chaque client.

⁵ IFRAH L., L'Information et le renseignement par Internet. Comment gérer l'information à l'heure du Web 2.0 ?, Que sais-je ?, n° 3881, PUF, 2010.p 157



Toutefois, il est important de souligner que les données personnelles sont sensibles et doivent être protégées contre toute utilisation abusive. C'est pourquoi il existe des lois et des réglementations qui encadrent la collecte, l'utilisation et la protection des données personnelles.

Il est également important de veiller à ce que les individus soient informés de la manière dont leurs données seront utilisées et qu'ils aient la possibilité de donner ou de retirer leur consentement à tout moment.

En résumé, les données personnelles sont un élément central du big data et peuvent être utilisées pour obtenir des insights sur les individus et améliorer les opérations commerciales. Toutefois, il est important de veiller à la protection de ces données et à respecter les lois et réglementations en vigueur en matière de protection de la vie privée.

1.2.2. L'importance du big data :

Le Big Data est une source privilégiée de données d'apprentissage pour la machine Learning. Il permet d'accélérer la courbe d'apprentissage et la précision des réponses. En effet, plus il y'a de données pour l'apprentissage, meilleurs seront les résultats. L'inverse est également vrai, moins il y'a de données pour l'analyse, moins les résultats seront précis et pertinents. Pire, en utilisant des données parcellaires ou préfiltrées, même issues du Big Data, de nombreux biais algorithmiques et statistiques peuvent aboutir à des résultats totalement erronés.⁶

Dans une perspective utilitariste, réglementer le Big Data suppose un examen, d'un côté, des avantages qu'il procure au plus grand nombre, de l'autre, des atteintes qu'il peut provoquer à des intérêts protégeables. Qu'il s'agisse des juristes ou des économistes, nul ne conteste les bénéfices considérables qu'apporte le traitement plus rapide et à un moindre coût de mégadonnées et la valeur économique qu'il représente dans tous les secteurs de la vie économique, sociale et culturelle. Ces bénéfices sont largement soulignés par la plupart des auteurs.⁷

Le big data nécessite aussi une infrastructure de calcul et de stockage de grande envergure pour gérer sa quantité et diversité. Le big data pose aussi des défis éthiques et de protection de la vie privée, car il peut impliquer la collecte et utilisation de données personnelles sensibles. Il est important de veiller à ce qu'il soit utilisé de manière responsable et respectueuse des droits des individus.

⁶ Frédéric-Jérôme PANSIER – Ijudge, vers une justice prédictive – LGM Edition 2019, p 33

⁷ Le big data et Droit. G'Sell, Florence- DALLOZ 2020. p 9-10



En conclusion, le big data est un phénomène complexe qui a un impact significatif sur de nombreux aspects de notre vie quotidienne. Il peut être utilisé pour améliorer les opérations commerciales, optimiser les processus de prise de décision et obtenir de meilleures insights sur les clients et les marchés, mais il faut le gérer de manière éthique et responsable.

2. Le cadre juridique et institutionnel assurant la protection des données personnelles et Big-data au Maroc :

Au Maroc, la protection des données personnelles est assurée par la loi 09-08 qui définit les principes et les obligations en matière de traitement des données personnelles. Cette loi crée également une Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel, chargée de veiller à l'application de la loi et plusieurs missions. Sans oublier d'autres institutions assurant le renforcement de cette protection. Et c'est ce que nous allons traiter ci-dessus.

2.1. Le cadre juridique des données personnelles et du Big-data au Maroc :

L'établissement d'un cadre juridique bien défini ainsi que la mise en place de mécanismes de contrôle performants sont des éléments primordiaux pour instaurer un équilibre optimal entre la sécurité et la protection des droits et libertés fondamentaux dans le cadre d'une politique de préservation des données personnelles.

2.2. L'arsenal juridique protégeant les données personnelles et les big data :

La protection des données personnelles est en constante évolution. Il existe plusieurs textes nationaux qui sont mis en place pour cela, notamment (classés par ordre d'importance juridique):

❖ La constitution

L'article 24 de la Constitution de 2011 sacrifie le droit à la protection de la vie privée. En effet, la réforme constitutionnelle de juillet 2011 a réitéré la ferme volonté du Royaume du Maroc de bâtir un État de droit, démocratique et moderne, consacrant les droits de l'Homme ainsi que les libertés individuelles et collectives. Parmi ces derniers, le droit à la protection de la vie privée s'érite en un pilier fondamental.

La Constitution souligne ce droit fondamental en ces termes : « Toute personne a droit à la protection de sa vie privée...les communications privées, sous quelque forme que ce soit, sont secrètes. Seule la justice peut autoriser, dans les conditions et selon les formes prévues par la



loi, l'accès à leur contenu, leur divulgation totale ou partielle ou leur invocation à la charge de quiconque ».⁸ La Constitution vise à garantir les droits des individus sur les informations personnelles en affirmant le principe de protection de la vie privée.

❖ **La loi 09-08 sur la protection des données personnelles.**

La loi 09-08 sur la protection des données personnelles vise à protéger les droits des individus en ce qui concerne l'utilisation de leurs informations personnelles. Elle a été mise en place pour encourager le développement du secteur tertiaire au Maroc, en permettant la délocalisation d'activités du secteur en provenance d'Europe.

Conformément aux dispositions légales, il est exigé que les données à caractère personnel soient recueillies et traitées avec responsabilité et respect des droits fondamentaux de l'homme. La loi prévoit ainsi la protection des droits des individus concernés tout en imposant des obligations aux responsables de la collecte de ces informations. En outre, une confidentialité rigoureuse doit être assurée quant aux données collectées.

Une autorité de contrôle indépendante a été mise en place pour veiller à la conformité avec la loi 09-08. Des sanctions sont prévues en cas de violation de la loi.

Il est à noter que les données collectées dans le cadre des activités de défense et de sécurité ne sont pas couvertes par la loi 09-08. Cependant, il est possible que l'article 24 de la Constitution puisse offrir une protection supplémentaire pour les données personnelles dans ce contexte.

❖ **La loi 53-05 relative à l'échange des données électroniques⁹**

La loi 53-05 relative à l'échange des données électroniques régit les modalités d'échange des données d'ordre juridique par voie électronique. Elle établit un régime spécifique applicable aux données juridiques échangées par ce moyen, en particulier en matière de chiffrement et de signature électronique. Elle vise ainsi à garantir la fiabilité et l'intégrité des informations échangées.

En outre, la loi précitée définit le cadre juridique applicable aux opérations réalisées par les prestataires de services de certification électronique. Ces derniers sont tenus de respecter des règles strictes afin d'assurer la sécurité et la fiabilité des certificats électroniques délivrés aux titulaires. Les détenteurs desdits certificats sont également soumis à des obligations

⁸ L'article 24 de la constitution Marocaine

⁹ La loi sur l'échange électronique des données juridiques, n° 53-05, a été promulguée par Dahir du 30 novembre 2007, Bulletin Officiel n° 5584.

particulières visant à préserver l'intégrité et la confidentialité des informations échangées par voie électronique.

Ainsi, la loi 53-05 vise à encadrer et à sécuriser les échanges de données électroniques, en fournissant un cadre juridique précis et adapté aux spécificités de ce mode de communication. Elle permet ainsi de renforcer la confiance dans les échanges commerciaux et juridiques réalisés par voie électronique, en offrant un niveau de sécurité équivalent à celui des échanges traditionnels sur support papier. En outre, elle favorise le développement des nouvelles technologies de l'information et de la communication, en offrant un cadre légal sûr et fiable pour les échanges de données électroniques.

❖ **La stratégie nationale pour la société de l'information, dite « Maroc numérique 2013 »¹⁰:**

La stratégie nationale pour la société de l'information, appelée "Maroc numérique 2013", vise à mettre à jour le cadre législatif en matière de sécurité informatique et de sensibiliser le public aux dangers de la criminalité liée aux nouvelles technologies. Elle prévoit également la création de la Direction Générale de la sécurité des systèmes d'informations (DGSSI) pour renforcer la sécurité informatique au Maroc.

2.3. L'arsenal juridique protégeant le Big Data

Dans la majorité des États, les démarches relatives aux projets Big Data sont soumises au régime juridique en vigueur portant sur des enjeux tels que la sauvegarde de la vie privée et des renseignements personnels. De surcroît, les dispositions légales relatives à la préservation des données prescrivent que les principes actuels de protection des données soient maintenus.

Au Maroc la protection de Big-Data se réfère à la réglementation générale relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les données massives, à la différence des données personnelles, ne bénéficient pas d'une protection juridique spécifique. Elles constituent un champ attractif en matière de recherche et d'innovation dans divers domaines. Ce qui justifie l'ébauche d'un droit prospectif.

La réglementation en vigueur se focalise sur les intérêts particuliers et les droits fondamentaux tels que la préservation de la vie privée et la protection des données, lesquels reposent sur la notion de "données personnelles" permettant d'identifier ou de caractériser une personne

¹⁰ Le plan Maroc Numérique 2013 s'articule autour de quatre axes : favoriser l'accès à l'internet et à la connaissance, développer le programme e-gouvernement, améliorer l'informatisation destinée aux petites et moyennes entreprises afin d'accroître leur productivité, et soutenir les acteurs TI locaux ou exerçant en offshore.

physique. Toutefois, les processus de Big Data transcendent l'unique gestion et traitement de données à l'échelle individuelle, en incluant de plus en plus l'utilisation de données consolidées, de profils génériques et de profils de groupe. Dès lors, il convient de s'interroger sur la pertinence de la focalisation sur l'individu et les données personnelles à l'ère de Big Data. Les corrélations statistiques et les profils de groupe ne sont pas reconnus comme des données personnelles, malgré leur capacité à influencer largement le contexte de vie des individus. Qui plus est, la montée en puissance de l'usage de Big Data pose des interrogations quant à la définition même des données personnelles.

3. Le cadre institutionnel de la protection des données personnelles et du Big-data au Maroc :

Cette partie met en évidence l'importance des institutions dans la protection des données personnelles et du big data. Les institutions ont pour rôle de mettre en place un cadre juridique clair pour réglementer le traitement des données, de surveiller la conformité à la loi pour garantir la sécurité et la confidentialité des données, de sensibiliser le public aux enjeux de la protection des données, de former les professionnels impliqués dans le traitement de ces données, de sanctionner les violations de la loi et de défendre les droits des personnes concernées par le traitement des données personnelles.

3.1. La CNDP

La Commission Nationale de contrôle de la protection des données à caractère personnel (CNDP) est une organisation indépendante créée par la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel au Maroc. Elle a pour mission principale de garantir la protection des données personnelles en veillant à la mise en œuvre et au respect des dispositions de cette loi et des autres textes de référence en la matière.

Afin d'accomplir sa mission, la CNDP dispose d'un ensemble de prérogatives et de pouvoirs. Elle est notamment chargée de contrôler les traitements de données à caractère personnel effectués sur le territoire marocain, de vérifier la conformité de ces traitements avec les dispositions de la loi et des autres textes applicables, et de sanctionner les infractions éventuelles. La CNDP est également en charge de la sensibilisation et de l'information des utilisateurs concernant leurs droits en matière de protection de leurs données personnelles. Elle est ainsi chargée de leur offrir un mécanisme de plainte en cas de violation de ces droits.



Par ailleurs, la CNDP joue un rôle de veille en matière de protection des données à caractère personnel au Maroc. Elle est habilitée à produire des avis et des recommandations en la matière, ainsi qu'à formuler des propositions de réformes législatives et réglementaires.

Enfin, la CNDP est investie de missions transversales, qui lui permettent d'assurer une coordination efficace avec les autres acteurs concernés par la protection des données personnelles. Ainsi, elle est en charge de la coopération internationale en matière de protection des données, ainsi que de la formation et de la sensibilisation des différents acteurs impliqués dans les traitements de données à caractère personnel, qu'ils soient publics ou privés.

En somme, la CNDP est une institution clé pour la protection des données à caractère personnel au Maroc. Elle est chargée de veiller à la mise en œuvre des dispositions législatives et réglementaires en la matière, ainsi qu'à la sensibilisation et à l'information des utilisateurs. Elle dispose de pouvoirs importants pour sanctionner les infractions et proposer des réformes législatives et réglementaires. En tant qu'organisation indépendante, elle est garante de la protection des données personnelles au Maroc.

- L'information et sensibilisation
- Le Conseil et proposition
- La protection et traitement des plaintes
- Contrôle et investigation
- Veille juridique et technologique

La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) revêt une importance primordiale dans le dispositif marocain de préservation des données personnelles. En effet, elle assume un rôle essentiel dans le traitement des requêtes et déclarations émanant des responsables de traitement des données à caractère personnel.

Au-delà de cette mission, la CNDP est dotée d'une prérogative d'exception qui lui confère la possibilité d'autoriser la conservation desdites données au-delà des délais légaux prévus. En outre, elle est habilitée à délivrer des autorisations de traitement pour les données jugées sensibles. En somme, elle est responsable de la gestion du registre national de la protection des données personnelles, document qui consigne la liste exhaustive des fichiers traités par les autorités publiques, ainsi que les autorisations de traitement correspondantes.



Il ressort ainsi que la CNDP occupe une position centrale dans l'application de la loi n°09-08 relative à la protection des données à caractère personnel, étant garante de la protection effective des droits des personnes concernées.

3.2. La direction générale de la sûreté nationale :

La Direction Générale de la Sûreté Nationale (DGSN) a mis en place une stratégie pour lutter contre les crimes liés aux nouvelles technologies. Pour ce faire, la DGSN a créé plusieurs structures centrales telles que le Service de lutte contre la criminalité liée aux NTIC et le Service de lutte contre la cybercriminalité. En outre, des brigades spécialisées et des laboratoires régionaux ont été mis en place pour une réponse décentralisée.

La DGSN s'efforce également d'améliorer ses ressources humaines et matérielles. Elle recrute de plus en plus de profils spécialisés en cybercriminalité et cyberdéfense, et a renforcé son équipement pour s'adapter aux exigences de l'informatique légale.

En 2015, lors d'un séminaire, la DGSN a présenté un aperçu des infractions les plus courantes au Maroc qui peuvent compromettre la protection des données personnelles des citoyens. Les infractions les plus fréquentes comprennent les atteintes aux personnes, les fraudes bancaires et les attaques aux systèmes d'information. La DGSN travaille donc pour protéger les citoyens contre ces types de crimes en utilisant les dernières technologies et en formant son personnel.

3.3. La Direction Générale de la Sécurité des Systèmes d'Information :

La Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a pour vocation de coordonner les ministères et organismes compétents en vue de définir une stratégie nationale de sécurité des systèmes d'information. Elle s'attelle à proposer des normes et des standards de sécurité, à superviser l'octroi des autorisations relatives à l'utilisation de certificats électroniques, ainsi qu'à accompagner les acteurs publics et privés dans la mise en place de mesures de sécurité adéquates. La DGSSI s'emploie également à effectuer des audits de sécurité pour le compte des entités publiques, à mettre en place un dispositif de surveillance, de détection et de réaction aux attaques informatiques, ainsi qu'à assurer une veille technique pour anticiper les menaces et proposer des améliorations pertinentes. Enfin, la DGSSI assume un rôle prépondérant dans la sensibilisation des employés du secteur public aux enjeux liés à la sécurité des systèmes d'information, à travers la mise en place de formations et de campagnes de sensibilisation appropriées.



Par ailleurs, la DGSSI a pour mandat de garantir la sécurité des systèmes d'information de l'Etat, des entreprises et des citoyens contre toute forme de cyberattaque. Elle se doit de protéger les données personnelles, les infrastructures critiques, ainsi que l'ensemble des systèmes d'information, et de sensibiliser les citoyens et les entreprises aux risques inhérents à la sécurité des systèmes d'information. En outre, elle veille à coordonner les efforts de cybersécurité entre les différents acteurs du secteur public et privé, et à coopérer avec les autorités compétentes dans la lutte contre la cybercriminalité, en vue d'identifier et de poursuivre les auteurs d'infractions cybernétiques.

Conclusion

Il est important de protéger les données personnelles dans l'ère du big data car ces données peuvent être utilisées de manière abusive. Elles peuvent être utilisées pour cibler les utilisateurs avec de la publicité ou du contenu en ligne qui peut être invasif ou trompeur, ou elles peuvent être utilisées par des tiers à des fins de fraude ou de harcèlement.

En outre, si les données personnelles ne sont pas correctement protégées, elles peuvent être exposées à des risques de fuite ou de piratage, ce qui peut entraîner des dommages pour la vie privée et la réputation des personnes concernées¹¹.

Donc il est très important de protéger les données personnelles car cela peut contribuer à renforcer la confiance des utilisateurs dans l'utilisation de technologies en ligne et à favoriser un environnement numérique plus sûr pour tous.

La protection des données personnelles est devenue cruciale à l'ère du big data en raison de la quantité croissante de données qui sont collectées et utilisées par les entreprises et les organisations. Si les données personnelles ne sont pas correctement protégées, elles peuvent être utilisées de manière abusive pour cibler les utilisateurs avec de la publicité ou du contenu en ligne qui peut être invasif ou trompeur, ou elles peuvent être exposées à des risques de fuite ou de piratage. Cela peut entraîner des dommages pour la vie privée et la réputation des personnes concernées, ainsi que pour la confiance des utilisateurs dans l'utilisation de technologies en ligne.

¹¹ KAPLAN D., Informatique, libertés, identités, Éditions FYP, Fing #8, 2010. p 168.



Il est très important que les données personnelles soient protégées adéquatement pour prévenir ces risques et garantir la confiance des utilisateurs. Cela nécessite la mise en place de lois et de règlements qui réglementent la collecte, l'utilisation et la protection des données personnelles, ainsi que le respect de ces lois et règlements par les entreprises et les organisations. Ces dernières doivent également être transparentes quant à leur utilisation des données personnelles et prendre des mesures pour protéger adéquatement ces données.

En outre, les principaux apports de la recherche sur la protection des données personnelles dans l'ère du big data incluent la promotion de la transparence et de la responsabilité, la promotion de l'innovation et du développement économique et la protection de la vie privée des individus et la prévention des discriminations liées à l'utilisation abusive des données. En fin de compte, la recherche sur la protection des données personnelles peut aider à garantir que les individus ont le contrôle sur leurs propres informations et qu'elles sont utilisées de manière éthique et responsable.

Cependant, les limites de la recherche incluent le manque d'accès à des données fiables et à des informations précises sur les pratiques de collecte et d'utilisation des données personnelles par les entreprises et les organisations, ainsi que la variabilité de la réglementation en matière de protection des données d'un pays à l'autre.

Enfin, elle peut promouvoir la transparence et la responsabilité en obligeant les entreprises et les organisations à être claires sur la manière dont elles collectent et utilisent les données personnelles.



BIBLIOGRAPHIE

- AKKOUR, S. (2021). Droit et révolution numérique : Pour une reconfiguration des paradigmes entre Droit et Technique. *Revue Internationale des sciences Juridiques, Économiques et Sociales*, 2.
- Association des Utilisateurs des Systèmes d'Information au Maroc en collaboration avec la société SOLUCOM, Livre Blanc Données à caractère personnel : Quels enjeux et comment se préparer à la loi 09-08 ?
- Aurélie Banck & Catherine Schultis. (2018). *Vade-mecum de la protection des données personnelles pour le secteur bancaire et financier*, RB édition.
- Banck & Aurélie. (2019). RGPD : la protection des données à caractère personnel : Intègre l'ordonnance adaptant la loi Informatique et Libertés Ed.2, Editeur Gualino.
- BENSOUSSAN, A. (2010). *Informatique et libertés*, coll. Mémento, 2^eme éd., Francis Lefebvre.
- COUNCIL OF EUROPE - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, convention 108.
- CNIL. (2010). Rapport annuel. La Documentation française.
- C. Pierre-Beaux. (2005). *La protection des données personnelles* : Éd. Promoculture.
- David Forest, *Droit des données personnelles*, Gualino, lextenso éditions.
- Fabrice Mattatia. (2018). *RGPD ET DROIT DES DONNÉES PERSONNELLES*, 3^eme édition, Enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi Informatique et libertés de 2018.
- Frédéric-Jérôme PANSIER. (2019). *Ijudge, vers une justice prédictive* – LGM Edition.
- G'Sell & Florence. (2020). *Le big data et Droit*, DALLOZ
- HAOUNANI Amine. (2019). *L'utilisation des données personnelles dans le droit comparé* – mémoire pour l'obtention du Master Droit du Numérique – Sous la direction du professeure AKKOUR Soumaya Présenté et soutenue publiquement au seins de la FSJES/Settat.
- Hervé & Christian & Stanton-Jean & Michèle. (2018). *Innovations en santé publique : des données personnelles aux données massives (big-data)* Ed.1. DALLOZ
- IFRAH, L. (2010). *L'Information et le renseignement par Internet. Comment gérer l'information à l'heure du Web 2.0 ? Que sais-je ?, n° 3881*, PUF.
- ITEANU, O. (2008). *L'Identité numérique en question*, Eyrolles.



- Jessica Eynard. (2013). Les données personnelles, Quelle définition pour un régime de protection efficace ? Michalon Editeur.
- KAPLAN, D. (2010). Informatique, libertés, identités, Éditions FYP, Fing #8.
- La loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- La loi sur l'échange électronique des données juridiques, n° 53-05, a été promulguée par Dahir du 30 novembre 2007, Bulletin Officiel n° 5584.
- La Nouvelle constitution Marocaine. (2011).
- LEMOINE, P. (1999). Commerce électronique, Marketing et Libertés, Cahier Laser n° 2, Descartes et Cie.
- LEPAGE, A. (2002). Libertés et droits fondamentaux à l'épreuve de l'Internet : droits de l'internaute, liberté d'expression sur l'Internet, responsabilité, Litec.
- LUCAS, A. & DEVÈZE J. & FRAYSSINET J. (2001). Droit de l'informatique et de l'Internet, Collection Thémis Droit privé, PUF.
- L'HARMATTAN. (2008). La Sécurité de l'individu numérisé. Réflexions prospectives et internationales.
- MAISL, H. (1996). Le Droit des données publiques, LGDJ.
- MARIE-LAURE LAFFAIRE. (2005). Protection des données à caractère personnel : Éd D'organisation.
- Mattatia & Fabrice. (2013). Traitement des données personnelles : Le guide juridique - La loi Informatique et libertés et la CNIL - Jurisprudences Ed 1, Editeur: Eyrolles.
- Nathalie WALCZAK. (2014) La protection des données personnelles sur l'internet : Analyse des discours et des enjeux sociopolitiques. Thèse de doctorat en Sciences de l'information et de la communication Sous la direction d'Isabelle GARCIN-MARROU et de Franck REBILLARD.
- Rapport sur la protection des données personnelles dans le cadre du secteur de la sécurité au Maroc. (2015). Séminaire DCAF-CEDHD 19 et 20 octobre 2015- Rabat, Maroc.
- VIVANT, M. & VIVANT, dir. (2010). Lamy droit de l'informatique et des réseaux, éd. Wolters Kluwer.