Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 6 : Numéro 3

LA PROTECTION DES DONNEES PERSONNELLES AU MAROC: LE SYSTÈME JURIDIQUE ET INSTITUTIONNEL

THE PROTECTION OF PERSONAL DATA IN MOROCCO: THE LEGAL AND INSTITUTIONAL SYSTEM

AMRANI ANAS
Doctorant au CEDOC
Faculté des Sciences Juridiques, Economiques et Sociales - Oujda
Université Mohammed Premier
Laboratoire des Etudes et Recherches Juridiques Administratives et Politiques (LERJAP)
MAROC

TAIBI ZAHREDDINE
Professeur d'enseignement supérieur
Faculté des Sciences Juridiques, Economiques et Sociales - Oujda
Université Mohammed Premier
Laboratoire des Etudes et Recherches Juridiques Administratives et Politiques (LERJAP)
MAROC

Date de soumission : 06/08/2025

Date d'acceptation : 15/09/2025

Pour citer cet article :

AMRANI. A. & TAIBI. Z (2025) « Contribution à l'analyse de l'impact de l'automatisation des processus sur la pertinence du contrôle de gestion: Approche qualitative », Revue Internationale du chercheur «Volume 6 : Numéro 3» pp : 1085 - 1109

Résumé

La révolution technologique en train de se faire a des conséquences juridiques, surtout avec l'augmentation des crimes en ligne. Pour y faire face, plusieurs pays améliorent leurs lois sur la protection des données personnelles. La Déclaration universelle des droits de l'homme, adoptée en 1948, a reconnu le droit à la vie privée. Ensuite, l'OCDE a fait des recommandations et la Convention 108+ du Conseil de l'Europe a mis en place des règles plus précises. En 2019, le Maroc a adhéré à cette Convention, ce qui montre son engagement pour protéger les données personnelles, conformément à l'article 24 de sa Constitution. Pour garantir cette protection, il est nécessaire d'avoir des institutions chargées de réguler cette question efficacement. Dans cet article, nous allons expliquer comment les organismes assurent la protection des données personnelles, en mettant l'accent sur l'importance de la coopération entre ces institutions, ainsi que sur les liens entre les autorités nationales et internationales, dans un contexte où les échanges de données à l'échelle mondiale augmentent constamment.

Mots clés: Protection des données personnelles; vie privée; révolution technologique; cybercriminalité; Systèmes de Traitement Automatisé des Données STAD.

ABSTRACT

The ongoing technological revolution has legal consequences, especially with the rise of online crimes. In response, several countries are improving their laws on personal data protection. The Universal Declaration of Human Rights, adopted in 1948, recognized the right to privacy. Subsequently, the OECD made recommendations and the Council of Europe's Convention 108+ established more precise rules. In 2019, Morocco joined this Convention, demonstrating its commitment to protecting personal data, in accordance with Article 24 of its Constitution. To ensure this protection, it is necessary to have institutions responsible for effectively regulating this issue. In this article, we will explain how organizations ensure the protection of personal data, highlighting the importance of cooperation between these institutions, as well as the links between national and international authorities, in a context where global data exchanges are constantly increasing.

Key words: Personal data protection; private data; technological revolution; cybercriminality; Automated Data Processing Systems.

Introduction

Les progrès technologiques récents ont eu un impact notable sur le droit, surtout grâce à l'augmentation des échanges et à la réduction des distances.

Ces changements ont aussi entraîné une augmentation inquiétante de la criminalité, notamment sous forme de cybercriminalité et d'attaques informatiques, souvent réalisées avec des outils comme les virus, le piratage ou la contrefaçon.

Pour combattre ces activités, plusieurs pays ont mis en place des lois plus strictes visant la protection des données personnelles. [CASSAR B., (2020) La modernisation du service public de diffusion du droit, vers l'instauration d'une législation plateforme, Dalloz actualité].

En 1948, la Déclaration universelle des droits de l'homme a été adoptée, incluant le droit au respect de la vie privée comme un droit fondamental.

En 1980, l'OCDE a publié des recommandations sur la protection des données, en réponse à l'usage croissant et à la puissance des ordinateurs dans le traitement des informations.

L'année suivante, le Conseil de l'Europe a approuvé la Convention 108 sur la protection des données, permettant ainsi d'intégrer le droit à la vie privée dans la législation européenne.

Dans ce contexte, le Maroc valorise la protection des données personnelles et des droits associés, et a signé la Convention 108+ du Conseil de l'Europe le 28 mai 2019, marquant ainsi son engagement envers des normes élevées.

Il devient ainsi le premier pays arabe, africain et musulman à être reconnu par la Conférence internationale des commissaires à la protection des données et à la vie privée lors de la 33e session, qui s'est tenue à Mexico en novembre 2011.

De plus, l'article 24 de la Constitution marocaine énonce des principes essentiels qui garantissent la protection de la vie privée et des droits individuels. Il précise que le droit à la vie privée permet à chaque personne de conserver son intimité et ses données personnelles en sécurité.

Le texte met aussi en avant l'importance du domicile en définissant des règles strictes pour les perquisitions, afin de s'assurer qu'elles sont conformes à la loi.

On insiste sur la nécessité de respecter la confidentialité des communications personnelles, en précisant que seul le juge, en suivant les lois en vigueur, peut accéder ou divulguer leur contenu. [BANCK A., (2023). RGPD: la protection des données à caractère personnel, Ed.5, Editeur Gualino].

En outre, en 2021, le Maroc a adopté la loi n° 53.21, qui a approuvé le protocole de révision de la Convention du Conseil de l'Europe 108+.

L'intérêt de notre sujet repose sur les efforts des organismes chargés de veiller à ce que les lois et règlements soient efficaces et bien appliqués.

Cela nécessite la présence et l'action de ces organismes, ainsi qu'une structure institutionnelle solide pour garantir que les droits liés à la protection des données personnelles soient réellement mis en œuvre.

La problématique centrale qui se pose concerne l'efficacité des lois qui encadrent ce sujet, afin de permettre une protection suffisante des données sensibles, ce qui nous amène à nous interroger sur plusieurs points importants:

❖Dans quelle mesure le cadre marocain (Constitution, article 24, lois 09-08, 07-03, 05-20, institutions) assure-t-il juridiquement et institutionnellement une protection sérieuse des droits des personnes, tout en respectant les impératifs de sécurité nationale face aux défis technologiques ? Quels organismes existent et comment travaillent-ils ainsi que leurs relations avec d'autres institutions ?

❖Comment les autorités nationales en charge de la protection des données coopèrent-elles avec leurs homologues internationaux, dans un monde où l'échange de données entre pays est de plus en plus fréquent ?

Pour aborder cette problématique et tenter de répondre à ces interrogations, nous adopterons dans ce contexte une approche combinant une étude épistémologique, une analyse et une méthodologie prédictive.

Elle inclura l'examen et la recherche sur l'importance cruciale de la protection des données personnelles ainsi que sur le cadre de la coopération entre les organismes concernés.

Dans un contexte international, cette étude dépasse les frontières des États et souligne la nécessité de la collaboration entre les organismes chargés de la protection des données à l'échelle mondiale.

À partir de ce constat, il est légitime de se demander comment les données personnelles sont protégées dans l'ère numérique, afin de mieux comprendre les exigences juridiques et institutionnelles **(1),** et d'analyser de manière plus pratique, en second lieu, l'impact du travail et de la coopération entre les institutions chargées de trouver un équilibre entre la sécurité de l'État et la protection des données personnelles **(2).**

Une analyse sera menée pour mettre en lumière les éléments qui rendent les obligations du gouvernement marocain un atout pour assurer la transparence et la responsabilité dans l'utilisation des données personnelles, dans le but de protéger la nation.

L'article se termine en suggérant des recommandations et des perspectives pour l'avenir.

1. Le cadre juridique de la protection des données personnelles dans l'ère numérique au Maroc:

Pour que cette recherche soit complète, il est important de bien expliquer les concepts clés liés à la protection des données personnelles.

Nous commençons par préciser les principes fondamentaux de la protection des données personnelles, qui constituent un domaine distinct du droit à la vie privée.

Dans l'ère numérique actuelle, la protection des données personnelles est devenue un sujet crucial.

Le Maroc a su relever ces défis en élaborant un cadre juridique et institutionnel solide visant à garantir la confidentialité, l'intégrité et la sécurité des données personnelles, ainsi qu'à lutter contre les cybermenaces.

Dans cette section, nous allons explorer ce cadre juridique marocain, en mettant l'accent sur les lois, les réglementations et les politiques qui encadrent la protection des données personnelles et la confidentialité en ligne.

De la loi sur la protection des données personnelles à la loi sur la cybercriminalité, nous allons découvrir les bases de ce système juridique, en expliquant son rôle essentiel dans la confiance des citoyens, des entreprises et des institutions dans le monde numérique d'aujourd'hui.

1.1 L'arsenal juridique de la protection des données personnelles:

Au Maroc, la loi pionnière n° 09-08, promulguée le 18 février 2009 (dahir n° 1 09 15), a pris effet le 15 novembre 2012.

Elle est relative à la protection des données personnelles et a introduit pour la première fois un ensemble de règles juridiques alignées sur le droit européen, notamment inspirées de la Directive Européenne n° 95/46/CE.

Cette loi définit les données concernées et les traitements, les droits des personnes, les obligations des responsables de traitement, les transferts internationaux ainsi que les sanctions (amendes allant de 10 000 à 300 000 dirhams, et des peines de prison allant de trois mois à un an).

Elle établit et met en œuvre les principes fondamentaux du traitement des données personnelles, tels que le respect de la vie privée, la transparence, la responsabilité et la sécurité des données.

Elle crée également la CNDP (Commission Nationale de Contrôle de la Protection des Données).

Dans cette partie, nous analysons l'efficacité et l'efficience de la loi n° 09-08 relative à la protection des données à caractère personnel.

- **La loi 09-08 sur la protection des données à caractère personnel**:

L'article 24 de la Constitution de 2011 met en évidence clairement le droit à la protection de la vie privée et explique quels sont les cas où ce droit peut être limité, selon la loi (article 27). En effet, la réforme constitutionnelle de juillet 2011 a renforcé la volonté du Royaume du Maroc de construire un État de droit, démocratique et moderne. Elle reconnaît les droits de l'Homme ainsi que les libertés individuelles et collectives. Parmi ces libertés, le droit à la protection de la vie privée est un pilier essentiel. La Constitution souligne ce droit en disant: «Toute personne a le droit de protéger sa vie privée… les communications privées, sous n'importe quelle forme, sont secrètes. Seul un juge peut autoriser, dans les conditions et selon les procédures fixées par la loi, la consultation, la divulgation totale ou partielle ou l'utilisation de ces communications contre quiconque…». (Article 24 de la Constitution marocaine de 2011). L'objectif de la Constitution est de garantir les droits des citoyens concernant leurs informations personnelles en affirmant la protection de leur vie privée. Dans ce contexte, le législateur marocain a adopté la loi 09-08 relative à la protection des données à caractère personnel, afin de protéger les droits fondamentaux des individus lors du traitement de leurs données personnelles. Cette loi définit les responsabilités des personnes en charge du traitement des données, les droits des personnes concernées ainsi que les sanctions en cas de non-respect. Selon cette loi, les données doivent être collectées de manière légale, transparente et proportionnée, et les individus doivent être informés de l'usage qui sera fait de leurs données. La loi exige également que ces données soient sécurisées et préservées contre tout accès non autorisé. Les personnes concernées ont le droit de consulter leurs données, de les corriger ou de les supprimer. Des sanctions sont prévues contre les violations de la vie privée, la collecte illégale de données ou le manque de conformité aux règles de protection des données. Il convient de souligner que cette loi constitue une avancée importante dans le domaine de la protection de la vie privée et des données personnelles, à la lumière des évolutions technologiques dans un environnement numérique en constante transformation.

Ces évolutions ont affecté ce droit de manière qui pourrait être menacée si une régulation adéquate n'est pas en place concernant l'utilisation, le traitement, la diffusion et la conservation des données personnelles. L'utilisation des données personnelles doit s'appuyer sur une base juridique solide et comporter des mesures visant à protéger les utilisateurs contre toute atteinte à leurs données et à leur vie privée, afin de leur faire confiance dans les technologies de l'information et de la communication.

Une donnée personnelle est toute information qui permet d'identifier directement ou indirectement une personne physique.

Selon la définition juridique, il s'agit de toute information concernant une personne physique, qu'elle soit identifiable ou non, et qui peut être reconnue directement ou indirectement grâce à un élément comme un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou d'autres indices liés à son identité, ses actions ou son mode de vie. Le législateur marocain a également défini les données à caractère personnel dans l'article 1 de la loi 09 08. Selon cette loi, il s'agit de toute information, quel qu'en soit le format ou le support, comme le son ou l'image, concernant une personne physique identifiée ou identifiable, appelée la «personne concernée». On considère qu'une personne est identifiable si elle peut être reconnue directement ou indirectement, notamment grâce à des éléments comme un numéro d'identification ou des données liées à son identité physique, psychologique, génétique, économique, culturelle ou sociale. Les données à caractère personnel comprennent des informations numériques ou physiques relatives à une personne, comme son prénom, son nom, sa photo, sa date de naissance, son numéro de carte bancaire, ses données sociales, ses empreintes digitales, sa voix, etc. Parfois, ces données sont classées comme «données sensibles», ce qui signifie qu'elles révèlent des informations comme l'origine ethnique ou raciale, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, ou encore des données de santé, y compris génétiques. Collecter, enregistrer, conserver, transmettre, diffuser ou effacer ces informations relève des actions liées aux données personnelles. Cette loi traite aussi d'autres sujets, comme le transfert des données vers d'autres pays, le Registre national de protection des données, qui impose des obligations précises pour la création, l'utilisation ou la gestion des fichiers, ainsi que les sanctions, expliquées dans le chapitre VII. Le législateur marocain, dans le cadre du titre VII de la loi 09-08, a adopté des règles visant à protéger chaque individu contre l'utilisation de ses données personnelles par l'organisme responsable, qu'il s'agisse d'une personne physique ou morale. Ces règles visent à garantir que toutes les actions, du début à la fin, soient effectuées en

garantissant le bien-être de la personne concernée. Cette loi est le fondement de la régulation actuelle, mais elle ne couvre pas certains droits introduits par le RGPD[1] (portabilité, oubli, limitation du traitement, obligations de notification des violations, rôle du DPO[2], etc.).

Le RGPD exerce une influence majeure sur le système marocain, en substance et en incitation à renforcer la loi 09-08 et les pratiques internes, notamment via les efforts de la CNDP et les entreprises concernées.

1.1.1 La protection des systèmes de traitement automatisé des données:

Le Maroc a renforcé sa législation concernant les systèmes de traitement automatisé des données grâce à la loi n° 07-03. Cette loi marque une étape importante pour le Royaume. Elle ne concerne pas seulement des cas spécifiques, mais complète le code pénal et couvre de nombreux comportements illégaux liés à l'informatique. Les principales infractions définies dans cette loi sont liées aux intrusions et aux atteintes aux systèmes de traitement automatisé des données.

- **La loi 07-03 relative aux STAD**[3]

Le législateur marocain a pris des mesures proactives en adoptant la loi 07-03 sur les atteintes liées aux systèmes de traitement automatisé des données. Cette loi complète le code pénal avec des dispositions relatives aux infractions liées à l'informatique, en suivant une approche similaire à celle de la loi 09-08. Adoptée en 2003, cette loi est la première au Maroc concernant la cybercriminalité. Elle s'inspire notamment de la loi française dite loi GODFRAIN, adoptée le 5 janvier 1988. Elle traite des attaques informatiques ainsi que des violations des données numériques. Elle aborde également les systèmes de régulation et les sanctions disciplinaires. Cette législation met en lumière l'importance de distinguer l'accès aux données personnelles de leur conservation incorrecte. On peut ainsi distinguer deux types d'accès non autorisé : ceux qui proviennent de l'extérieur du système et ceux qui proviennent de l'intérieur. L'accès à un système informatique est défini comme une entrée non autorisée, ce qui constitue une intrusion illégale et trompeuse. [IFRAH L., (2010). L'information et le renseignement par Internet. Que sais-je ?, n° 3881, PUF]. Ainsi, la loi explique clairement ce qui est considéré comme illégal lorsque quelqu'un parvient à entrer dans un ordinateur connecté à Internet depuis l'extérieur d'un réseau. Cette loi fait partie du code pénal

[1] Le Règlement Général sur la Protection des Données est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE).
[2] Le Délégué à la Protection des Données

[3] Le système de traitement automatisé de données

marocain, aux articles 607-3 à 607-11. Concernant l'accès non autorisé à partir d'un système de l'intérieur, la loi marocaine, notamment l'article 607-3, indique qu'une personne qui entre intentionnellement sans permission dans un système informatique peut être punie. Cet article précise que « toute personne qui reste dans tout ou partie d'un système informatique auquel elle a accès par erreur et sans droit peut encourir la même sanction». Il est important de noter que la loi prévoit une sanction plus sévère si l'accès ou l'intervention non autorisée causent une dégradation du système. L'article 607-3, alinéa 3, dit: «La sanction est doublée lorsque cela a conduit soit à la suppression ou à la modification des données dans le système informatique, soit à une panne dans son fonctionnement».

De plus, la loi prévoit une peine variant entre deux et cinq ans de prison, accompagnée d'une amende de 100 000 dirhams si la violation entraîne la modification ou la suppression des données du système informatique, ou provoque une altération de son fonctionnement. La sanction est encore plus sévère si l'acte est commis par un fonctionnaire ou un employé en exercice de ses fonctions. La loi 07-03 considère également comme une atteinte toute action pouvant causer un dysfonctionnement temporaire du système, sa dégradation ou même son incapacité totale à fonctionner. Cela inclut notamment la modification des données, comme l'ajustement de tables dans une base de données, l'utilisation d'un moteur de recherche pour déplacer un serveur web, ou le transfert d'un site web pour intégrer une image inappropriée, parmi d'autres exemples. Sans limiter les sanctions plus graves prévues par d'autres articles, comme le premier alinéa de l'article 607-3, la loi marocaine impose ces punitions. Dans le cadre de cette question cruciale liée à la protection des données personnelles dans l'ère numérique, il est essentiel d'analyser en profondeur les relations complexes entre les acteurs de la sécurité nationale et les systèmes de gestion et de protection des données au Maroc. Alors que le secteur numérique s'entrelace de plus en plus avec la sécurité nationale, un sujet important émerge: comment gérer et protéger les données personnelles, qui représentent l'intimité des individus, dans ce contexte. Les défis deviennent plus difficiles quand on doit trouver un équilibre entre les besoins de sécurité d'un État et les droits de chacun à la vie privée. Face à la problématique de la cybercriminalité, les approches légales varient d'un pays à l'autre. Cela s'explique, en partie, par l'émergence de deux tendances distinctes, chacune adoptant une perspective différente sur ce phénomène. Le premier courant pense qu'il n'est pas nécessaire de faire la différence entre les informations stockées sur des supports classiques et celles stockées de manière automatisée. Ainsi, la cybercriminalité ne justifie pas la mise en place de nouvelles dispositions législatives. Le deuxième courant considère la

cybercriminalité comme un phénomène spécifique qui exige l'adoption de nouvelles lois. Les réponses juridiques marocaines s'inscrivent dans cette vision, en reconnaissant la nécessité d'adopter des mesures spécifiques pour lutter contre ce phénomène en constante évolution.

1.1.2 L'arsenal juridique du cyberespace au Maroc:

La sécurité dans le numérique est devenue un sujet très important dans notre société qui évolue tout le temps.

Pour lutter contre les risques qui menacent les données et les systèmes informatiques, le Maroc a créé la loi 05-20 sur la cybersécurité.

Cette loi est très importante pour protéger le monde numérique marocain, en définissant des règles, des standards et des punitions pour éviter et combattre les attaques informatiques.

- **La loi 05-20 sur la cybersécurité**

La loi 05-20 vise à prévenir et à répondre aux menaces en ligne. Elle précise les rôles de chaque partie impliquée, comme les autorités publiques, les entreprises et les individus. Cette loi établit aussi des moyens de collaboration entre les différents acteurs de la sécurité des informations, pour adopter une approche globale en matière de cybersécurité. Une des bases de cette loi est la protection des données personnelles. Elle impose aux organisations publiques et privées de mettre en place des mesures de sécurité suffisantes pour garantir la confidentialité, l'intégrité et la disponibilité des données sensibles. De plus, elle fixe des règles pour signaler les incidents de sécurité, imposant aux acteurs de faire connaître toute situation pouvant mettre en danger les données personnelles. La loi 05-20 porte également une attention particulière à l'empêchement et à la punition des actes criminels en ligne. Elle rend illégaux des comportements comme le piratage, la fraude informatique, l'usurpation d'identité en ligne, et d'autres formes de cybercriminalité. Des sanctions sévères sont prévues pour dissuader les personnes ou groupes de commettre ces actes. Outre la prévention et la répression, la loi 05-20 met aussi l'accent sur l'éducation et la formation en cybersécurité. Elle encourage la mise en place de campagnes pour informer les utilisateurs des risques liés à Internet et promeut la formation des professionnels pour renforcer leurs compétences dans ce domaine en constante évolution. La loi prévoit également des mécanismes de travail entre les pays, les organisations internationales et le secteur privé, pour échanger des informations sur les nouvelles menaces et coordonner les actions afin de lutter contre la cybercriminalité à l'échelle mondiale. En conclusion, la loi 05 20 sur la cybersécurité marque un point important dans la protection du numérique au Maroc. En créant un cadre juridique clair, elle vise à développer la confiance des utilisateurs, à protéger les données et à prévenir les cyberattaques.

Cependant, il faut rappeler que la cybersécurité est un défi permanent, car les menaces évoluent constamment. Pour cela, la loi prévoit aussi des mécanismes réguliers d'évaluation et d'adaptation afin de suivre les progrès technologiques et les nouvelles formes de cybermenaces. Cette loi renforce encore davantage la collaboration entre le secteur public et le secteur privé concernant la sécurité informatique. Elle encourage les partenariats entre les organismes gouvernementaux et les entreprises pour faciliter l'échange d'informations et travailler ensemble pour repérer et répondre aux incidents de sécurité.

Cette collaboration entre différents acteurs est essentielle pour améliorer la résilience du réseau informatique du pays.

La loi 05-20 place aussi une grande importance sur la protection des infrastructures importantes comme les réseaux électriques, les systèmes de transport et les services de santé.

Elle impose des règles de sécurité spécifiques ainsi que des mesures de protection plus strictes pour garantir le bon fonctionnement des services essentiels et résister aux attaques possibles.

Il faut noter que cette loi ne se limite pas à la sécurité informatique nationale mais inclut aussi des dispositions sur la coopération internationale. Elle encourage activement le Maroc à participer à des initiatives mondiales visant à renforcer la sécurité informatique, notamment via des forums, des conférences et des programmes de partage d'informations. En résumé, la loi 05-20 sur la sécurité informatique représente une grande avancée pour le Maroc dans la protection du monde numérique contre les menaces en ligne. En établissant un cadre légal clair, en favorisant l'éducation et la formation, et en encourageant la coopération à l'intérieur du pays et à l'international, cette loi vise à accroître la confiance dans l'utilisation des technologies numériques et à assurer la protection des données, des infrastructures et des services essentiels. Cette situation demande une réflexion sérieuse sur les règles, les méthodes et les lois existantes, tout en mettant en lumière l'importance d'une bonne collaboration entre les services de sécurité et les organisations chargées de protéger les données personnelles. La protection des données sensibles, essentielle pour la stabilité et la sécurité des États, doit être accompagnée de lois et d'organismes qui garantissent le respect des droits de chaque individu. C'est dans ce cadre complexe que nous allons étudier les mécanismes qui régissent ces relations, afin de comprendre comment le Maroc a construit ses politiques pour équilibrer la sécurité nationale et la protection des droits fondamentaux dans un environnement numérique en constante évolution. Bien que la création d'une loi claire et adaptée ait permis d'établir une base solide pour protéger les données des citoyens au Maroc, il reste crucial d'ajouter des mesures garantissant une surveillance rigoureuse de l'application de ces lois et une protection

suffisante des données personnelles. Au Maroc, plusieurs institutions jouent un rôle essentiel dans la gestion et la protection des données personnelles. Ces organismes collaborent pour assurer la sécurité de l'État tout en veillant sérieusement aux droits fondamentaux des individus. En Europe, les principales organisations chargées de la protection des données et de la libre circulation des données sont le Conseil de l'Europe, la Commission Européenne et le Comité Européen de la Protection des Données (EDPB), qui a été créé le 24 mai 2018 et chargé d'assurer une application uniforme du RGPD, d'émettre des recommandations, des codes de bonne conduite et de résoudre les litiges transfrontaliers.

La Commission d'accès à l'information (CAI) du Québec est l'autorité en charge de la mise en œuvre de la Loi 25, avec des responsabilités de surveillance, d'enquête, de sanction et de juridiction administrative. Elle a un rôle central aussi bien pour les organisations publiques que privées, avec le pouvoir de rendre des décisions en tant que tribunal administratif.

En 2025, la CAI a été active, par exemple en interdisant une technologie de reconnaissance faciale jugée incompatible avec la vie privée, montrant ainsi son rôle régulateur concret. Les 27 États membres de l'Union européenne ainsi que les pays de l'Espace économique européen (Islande, Liechtenstein, Norvège) disposent d'une législation sur la protection des données et d'une autorité de supervision indépendante.

2. **Le Maroc a un système d'institutions solide pour protéger les données personnelles:**

Des organismes comme la Direction Générale de la Sureté Nationale, la Commission Nationale de contrôle de la protection des Données à caractère Personnel et la Direction Générale de la Sécurité des Systèmes d'Information contribuent à cette protection. Le pays s'engage à préserver la confidentialité, la sécurité et les droits des personnes dans l'espace numérique. Ce système d'institutions renforce la confiance des citoyens dans l'utilisation des services en ligne et favorise la création d'un environnement numérique sécurisé et responsable au Maroc.

- **Direction générale de la sureté nationale**

Établie conformément au Dahir n° 1. 56. 115 du 5 chaoual 1375 (16 mai 1956), la Direction Générale de la Sécurité Nationale (DGSN) a pour mission principale d'assurer le maintien de l'ordre public et de veiller à la protection complète des droits des individus ainsi que de leurs biens. Transformée en une institution centrale, elle a créé plusieurs organismes, parmi lesquels figurent la Direction de la lutte contre la criminalité liée aux nouvelles technologies et le Service de lutte contre la cybercriminalité, tous deux intégrés dans le domaine de la

police judiciaire. Le premier service est pourvu d'un laboratoire central des traces numériques, dédié à l'expertise des supports numériques saisis par les services de police à l'échelle nationale. Quant au deuxième service, il relève de la brigade nationale de la police judiciaire et dispose également de son propre laboratoire d'exploitation des traces numériques.

En outre, la DGSN compte 29 brigades spécialisées dans la lutte contre la cybercriminalité, dont quatre possèdent leurs propres laboratoires à Casablanca, Fès, Marrakech et Laâyoune.

Dans la lutte contre la cybercriminalité, l'élément humain formé et bien encadré demeure d'une importance capitale.

Afin de s'adapter en permanence à l'évolution de ce phénomène, la Police nationale marocaine a procédé au recrutement de profils de qualité.

Les équipes composant les différentes brigades sont constituées d'ingénieurs, de techniciens spécialisés, d'analystes, de juristes, ainsi que d'autres professionnels dont l'expertise renforce les actions menées dans ce domaine.

Le gouvernement s'engage à améliorer la formation pour que les forces soient plus attentives aux risques liés à la cybercriminalité. La DGSN a lancé des actions importantes et a fait beaucoup d'efforts pour faire face à la montée de la criminalité dans le domaine des nouvelles technologies. L'Autorité Judiciaire, qui défend les libertés individuelles, s'inscrit naturellement dans cette démarche. Elle agit comme un pilier essentiel pour équilibrer la sécurité et la protection des droits de chacun. Le Conseil Supérieur du Pouvoir Judiciaire au Maroc, qui est un organisme clé chargé d'améliorer le fonctionnement du système judiciaire, joue un rôle important dans la protection des données personnelles. Dans le cadre de son plan stratégique pour la période 2021-2026, le Conseil s'est engagé à renforcer la sécurité judiciaire tout en veillant à ce que les décisions soient prises rapidement et que les retards soient éliminés. L'objectif est aussi de renforcer la confiance des citoyens dans le système judiciaire. La sécurité judiciaire est un pilier essentiel de cette stratégie. Elle inclut la protection des informations personnelles. Le Conseil a mené plusieurs actions concrètes, comme la publication en ligne des décisions de la Cour de cassation et la diffusion de la jurisprudence. Ces mesures visent à améliorer l'efficacité du système judiciaire, mais elles favorisent aussi un lien de confiance entre la population et les institutions, basé sur le respect et l'écoute mutuelle. En tant que garant des libertés individuelles, le Conseil Supérieur du Pouvoir Judiciaire reconnaît la nécessité de protéger les données personnelles. Cette protection s'inscrit dans une approche globale et responsable de la gouvernance, qui comprend des mesures essentielles pour assurer la sécurité des informations. Cependant, il faut rappeler que

le Conseil ne s'occupe pas uniquement de la protection des données. Il a plusieurs responsabilités liées à l'efficacité du système judiciaire, comme la publication des décisions, l'amélioration de la qualité des jugements, et la création d'une relation de confiance entre les citoyens et l'institution. Même si la protection des données n'est pas son seul objectif, ses actions visant à renforcer la sécurité et la confiance dans le système judiciaire ont un impact indirect sur cette protection.

- **Direction Générale de la Sécurité des Systèmes d'Information**

Dans le Royaume du Maroc, comme en France, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a été crée au sein de l'Administration de la Défense Nationale. Elle relève de l'Administration de la Défense Nationale du Royaume du Maroc. Son rôle concerne la prévention et la détection des attaques informatiques.

La DGSSI a pour mission de coordonner les actions entre les différents ministères concernant la création et l'application de la stratégie nationale en matière de sécurité des systèmes d'information.

Elle s'assure que les décisions du comité stratégique sont bien appliquées, propose des règles et normes spécifiques pour la sécurité des systèmes d'information de l'État, délivre des autorisations et gère les déclarations liées à l'utilisation de la cryptographie. Elle est également en charge de certifier les outils utilisés pour créer et vérifier les signatures électroniques. Elle valide les entreprises qui fournissent des services de certification électronique conformément aux lois en vigueur. Elle accompagne et conseille les administrations publiques, les organismes et les entreprises privées dans la sécurisation de leurs systèmes d'information. De plus, elle développe son expertise scientifique et technique dans le domaine de la sécurité des systèmes d'information. Elle effectue des audits pour évaluer la sécurité des systèmes d'information des administrations et organismes publics. Elle met en place un système de surveillance, de détection et d'alerte face aux incidents qui menacent la sécurité des systèmes d'information de l'État, et elle coordonne les actions à entreprendre. En cas d'urgence ou de menace, elle informe le comité stratégique et effectue une veille technologique pour anticiper les évolutions et proposer les innovations nécessaires en matière de sécurité des systèmes d'information.

- **Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel**

La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) est une institution administrative indépendante créée par la loi 09-08 du 18 février

2009. Elle est composée de sept membres, dont un président et six autres, nommés par le roi après avoir été proposés par des institutions comme le Premier ministre ou les Chambres du Parlement. Leurs mandats sont d'une durée de cinq ans et peuvent être renouvelés une seule fois. Le but de la CNDP est de surveiller la gestion des données personnelles, d'informer le public et les organisations sur les droits et obligations liés à la protection des données, ainsi que de garantir le respect de la loi et des textes qui encadrent cette protection.

Parmi ses missions principales figurent le conseil des pouvoirs publics, l'instruction des plaintes, la gestion des déclarations, la tenue d'un registre public, le suivi des évolutions légales et technologiques, et les contrôles et enquêtes sur place.

La CNDP peut aussi accéder à des locaux, des données et des équipements et appliquer des sanctions administratives ou pénales si nécessaire.

La CNDP est la première institution au Maroc chargée de réguler les données personnelles et fonctionne de façon similaire à la CNIL en France.

Elle effectue des actions de sensibilisation auprès des individus, des organismes et des institutions publiques et privées pour leur faire comprendre leurs droits.

Pour cela, elle dispose d'un site internet et d'un portail électronique régulièrement mis à jour, ainsi que de brochures, de spots radiodiffusés et d'une émission radio hebdomadaire. La CNDP accompagne aussi les acteurs concernés pour assurer la conformité de leurs procédures de traitement des données. Elle porte une attention particulière aux secteurs qui traitent un nombre important de données personnelles. Son rôle inclut aussi de conseiller le gouvernement, le parlement et l'administration sur la protection des données. Elle peut émettre des avis sur des projets de lois, proposer de nouvelles législations au gouvernement et aider le Maroc dans les négociations internationales. La CNDP se charge également des plaintes des citoyens en cas de violation de leurs droits en matière de protection des données. Entre 2011 et 2015, le nombre de ces plaintes a été élevé, dans des domaines comme la publicité indésirable, les spams, et la vidéosurveillance. La CNDP reçoit aussi des demandes d'autorisation de traiter des données, notamment les données sensibles. Elle peut accorder des autorisations pour conserver des données plus longtemps ou traiter certaines données. Enfin, la CNDP gère un registre national des données personnelles, qui inclut la liste des fichiers traités par les autorités publiques ainsi que les autorisations données. Elle a le droit d'effectuer des enquêtes et des contrôles pour vérifier si les données sont traitées conformément à la loi. Ces contrôles peuvent entraîner des amendes ou des poursuites judiciaires. La CNDP suit aussi les évolutions légales et technologiques, observant les tendances qui pourraient affecter

la protection des données au Maroc. Cependant, son statut juridique est parfois critiqué, car bien qu'elle soit présentée comme indépendante, elle est sous la tutelle du gouvernement. Cela peut limiter son impartialité et son pouvoir réel par rapport aux normes internationales.

2.1. La collaboration et la coopération entre les institutions visent à trouver un équilibre entre la sécurité de l'Etat et la protection des données personnelles:

Les différentes institutions travaillent ensemble de manière étroite pour garantir la sécurité du pays tout en respectant les droits des citoyens. Il est essentiel d'équilibrer la protection des données personnelles et les responsabilités en matière de sécurité nationale. Pour cela, les organismes marocains ont mis en place des accords de coopération et de coordination afin de gérer et protéger correctement ces informations. Par exemple, ces protocoles comprennent la création d'un système de gestion de la sécurité des informations, qui surveille les politiques de sécurité et les procédures liées aux données sensibles.

Ils incluent aussi la création d'un système pour surveiller et détecter les incidents, la mise en place de règles pour gérer ces incidents, la création d'un système pour contrôler qui a le droit d'accéder aux données, ainsi que des protocoles pour sauvegarder les données et les récupérer en cas de problème.

De plus, il y a des tests et des audits réguliers, des accords entre les institutions gouvernementales et les autorités locales, ainsi que des accords avec des organisations internationales. Enfin, ils collaborent avec les entreprises privées pour améliorer la sécurité des données et se défendre contre les menaces informatiques. Des campagnes d'information ont aussi été organisées pour informer les citoyens et les entreprises sur les risques liés à la sécurité des données ainsi que les mesures à prendre pour prévenir ces risques. En effet, la relation entre les organismes chargés de la sécurité nationale et de la protection des données repose sur la coopération et la coordination. Ces institutions travaillent ensemble pour assurer la sécurité des citoyens tout en protégeant leurs droits et les intérêts de l'État. Pour mieux appliquer les mesures de protection des données personnelles, l'Institution du Médiateur du Royaume et la CNDP ont signé un accord le 16 décembre 2019. Cet accord définit un cadre qui renforce les relations entre les parties, notamment en ce qui concerne les droits des citoyens et le respect de la loi 09-08, en particulier pour les administrations publiques. La CNDP et le Ministère de l'Intérieur travaillent étroitement ensemble car leurs responsabilités concernent à la fois la protection des données et la sécurité nationale. La CNDP peut conseiller sur la protection des données, tandis que le Ministère de l'Intérieur est chargé d'obtenir et d'utiliser ces données pour la sécurité de l'État. Cependant, il faut noter que la loi

09-08 sur la protection des données personnelles inclut des règles qui définissent clairement le rôle limité de la Commission Nationale dans ce domaine. Ces règles montrent également que la Commission a plus d'indépendance, sans reproduire le système français. Cela lui donne un pouvoir davantage renforcé, lui permettant de faire respecter strictement les dispositions de cette loi. Les sanctions sont prises en charge par le procureur de la juridiction concernée, qui reçoit les observations.En ce qui concerne les accords et protocoles de coopération, ils ont été créés pour gérer efficacement les institutions. Par exemple, en 2019, une convention de collaboration entre la Présidence du Parquet et la CNDP a été signée. Cette convention, signée par le procureur général et le président de la CNDP, se base sur deux axes principaux: la gestion des plaintes, des dossiers et des signalements concernant les violations de la loi 09-08, ainsi que le partage d'expériences et de compétences en matière de formation.

Cette initiative a pour objectif de lutter contre toutes les formes d'atteintes aux données personnelles et de protéger la vie privée des citoyens.

De plus, une convention d'adhésion au programme DATA-TIKA[4] a été signée entre le MESRSI[5] et la CNDP.

Cette initiative montre l'engagement des parties concernées pour une utilisation responsable des données, témoignant d'une volonté commune de renforcer la protection. En outre, le CSPJ[6], la Présidence du Ministère Public, l'Institution du Médiateur du Royaume et la CNDP ont organisé, le 11 novembre 2022 à Rabat, une journée d'étude sur le cadre juridique de la protection des données personnelles et la bonne gouvernance. Dans son discours d'ouverture, le procureur général a souligné l'importance d'une coopération entre les parties pour appliquer efficacement les lois sur la protection des données. Le Ministère Public, chargé de protéger la vie privée des citoyens selon la loi, doit veiller à ce que ces règles soient respectées. Dans ce contexte, le CSPJ collabore étroitement avec le Ministère Public, le Médiateur du Royaume et la CNDP pour gérer efficacement les services publics et assurer une protection des données personnelles suffisante. Moulay El Hassan Daki, procureur général du Roi et président du Ministère Public, souligne l'importance de travailler ensemble pour améliorer la gouvernance et protéger les données personnelles. Il souligne que le Maroc, qui a inscrit le droit à la vie privée dans sa Constitution, doit faire face à des risques qui augmentent avec l'avancée des technologies. La loi 09-08, qui protège les données

[4] La confiance numérique
[5] Le Ministère de l'Enseignement supérieure, de la Recherche scientifique et de l'Innovation
[6] Le Conseil supérieur du Pouvoir judiciaire

personnelles, fixe les obligations du responsable du traitement et les droits des personnes concernées, offrant ainsi une réponse aux défis actuels. Le Ministère Public, en tant que figure centrale, a lancé des actions pour renforcer les compétences des juges. Il est important de dire que ces règles et normes évoluent constamment pour suivre les progrès technologiques et les nouvelles menaces en matière de cybersécurité. Les institutions marocaines continuent d'agir pour sécuriser les données et protéger les citoyens contre les risques liés à l'informatique.

Une bonne gestion des services publics est un pilier important pour les pays avancés, dans le contexte d'un État de droit et d'institutions solides.

Le Maroc met en avant la protection de la vie privée et les droits liés à celle-ci dans son engagement envers la coopération internationale.

C'est le premier pays arabe, africain et musulman à avoir été reconnu par la Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée, ce qui témoigne de son désir de travailler avec d'autres pays dans ce domaine.

L'Union européenne, en particulier via la Conférence des Directeurs Nationaux de la Protection des Données, a organisé une réunion à Rabat en 2018 pour comparer la loi marocaine 09-08 avec le RGPD et identifier les différences entre le Maroc et l'UE, ainsi que les méthodes d'échange d'informations.

Les entreprises marocaines, surtout celles qui manipulent les données des citoyens européens, sont encouragées à suivre les règles du RGPD pour rester compétitives et maintenir des relations commerciales stables avec l'UE. Les entreprises marocaines doivent respecter plusieurs exigences du RGPD, comme le consentement clair, le respect des droits des personnes, la sécurité des données et la preuve de conformité. Pour cela, elles doivent mettre en place des mécanismes stricts comme la cartographie des données, la sécurisation des informations, l'emploi d'un DPO (Délégué à la Protection des Données) et une réponse aux demandes dans un délai d'un mois. Les sanctions en Europe peuvent aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial, ce qui rend la non-conformité très risquée. Certains professionnels du droit, comme Me Ezzouate, demandent une révision de la loi marocaine afin qu'elle prenne en compte les évolutions technologiques, comme l'intelligence artificielle, les données massives et les objets connectés, et rattrape le retard législatif. Bien qu'il n'ait pas de pouvoir direct en Maroc, l'EDPB (Conseil européen pour la protection des données) influence indirectement les entreprises marocaines grâce à ses orientations juridiques et ses bonnes pratiques, qui servent de guide pour se conformer aux normes européennes. Cet impact indirect constitue un point d'union important. Le Maroc a signé un

accord de reconnaissance d'adéquation en alignant sa loi sur les exigences du RGPD, ce qui permet aux entreprises marocaines de transférer des données plus facilement vers l'UE. Le pays a également conclu des accords de coopération avec des pays comme les États-Unis, et promeut l'adoption de normes internationales. Ces accords incluent l'échange d'expériences, de bonnes pratiques et de systèmes collaboratifs pour résoudre les problèmes liés à la protection des données à l'international. L'application de ces normes aide à renforcer la législation du pays et facilite les échanges commerciaux avec d'autres pays.

Par exemple, le Maroc a signé des accords comme le RGPD de l'UE et participe à des normes établies par des organisations comme l'OCDE ou la Commission Internationale de l'Éclairage (CIE). L'objectif de ces normes est de créer des règles communes dans le domaine de la protection des données, ce qui simplifie les échanges à l'international.

En tant que secrétariat permanent du Réseau Africain des Autorités de Protection des Données Personnelles (NADPA/RAPDP)[7], le Maroc joue un rôle clé dans la promotion et la coordination des initiatives africaines visant à renforcer la protection des données personnelles.

Cette position montre son engagement à promouvoir la protection de la vie privée en Afrique et à participer activement aux discussions internationales.

2.2. Les obligations des gouvernements

Le gouvernement marocain doit s'assurer d'utiliser les données personnelles de manière transparente et responsable, afin de protéger le pays.

Bien qu'un cadre juridique solide existe, l'efficacité dépend de l'application concrète et de l'organisation.

Pour cela, il est important de:

- ✓ Elaborer une analyse d'impact sur la protection des données (DPIA): encore peu développée, mais nécessaire lorsqu'il s'agit de traitements pouvant représenter un risque pour les droits et libertés des personnes.

Le gouvernement et la CNDP doivent demander au responsable du traitement de faire une analyse d'impact sur la protection des données dès qu'un traitement peut entraîner un risque élevé pour les droits des citoyens.

[7] (Network of African Data Protection Authorities/Réseau Africain des Autorités de Protection des Données Personnelles)

- ✓ Désigner un DPO (Délégué à la protection des données), qui a un rôle essentiel dans la gestion de la confidentialité et de la sécurité des données personnelles au sein des entreprises.

  Dans un contexte où les données jouent un rôle central dans les activités, ce professionnel veille à ce que les pratiques internes respectent les lois comme la CNDP, et protègent ainsi les informations traitées.

  Ce rôle est encore peu développé dans les administrations et les entreprises.
- ✓ Réunir et tenir correctement les Registres des traitements: obligatoires, mais souvent absents ou incomplets.

  Une erreur courante est de ne pas documenter correctement chaque traitement de données.

  Certaines entreprises négligent cette étape, pensant que quelques notes suffisent.

  Une documentation incomplète peut rendre difficile la traçabilité des données personnelles et exposer l'organisation à des amendes lors d'un contrôle.
- ✓ Mettre en œuvre des mesures de sécurité: obligatoire, mais sans normes uniques ou certificats obligatoires.
- ✓ Notifier les violations de données: obligatoire par la loi, mais la culture de notification reste faible.
- ✓ Contrôler et sanctionner les non-respect des règles: peu fréquent, peu médiatisé, et nécessite un renforcement pour avoir un effet dissuasif.
- ✓ Préparer les contentieux: encore limité, il manque de jurisprudence claire et structurante.

  Le gouvernement doit être transparent concernant la collecte, le stockage et l'analyse des données personnelles.

  Cela peut inclure la publication régulière de rapports sur ces activités, l'information des citoyens sur les politiques de collecte et la mise en place de mécanismes d'enquête sur l'utilisation de leurs données.

  En adoptant ces pratiques responsables et transparentes, le gouvernement renforce la confiance des citoyens dans l'utilisation des données pour protéger le pays, tout en veillant à ce que cette utilisation soit conforme à la loi 09-08 sur la protection des données personnelles.

  Cela contribue à garantir que le gouvernement utilise les données de manière légitime et responsable, tout en préservant les droits fondamentaux des citoyens à la vie privée et à la protection de leurs données.

En conclusion, l'utilisation des données personnelles par les gouvernements pour protéger leur pays est une question complexe qui exige un équilibre entre la sécurité nationale et la protection des droits fondamentaux des citoyens.

Conclusion

En résumé, ces dernières années ont vu une prise de conscience grandissante des institutions gouvernementales sur l'importance de l'information, qui est aujourd'hui vue comme un élément important.

Ces changements ont entraîné des responsabilités majeures pour protéger les données personnelles, qui sont étroitement liées à la sécurité nationale et au bien-être de tous.

L'utilisation croissante des données, particulièrement dans des domaines comme la santé, la finance et les médias, crée un besoin urgent de renforcer les protections qui empêchent les atteintes à la vie privée et les menaces informatiques.

La technologie évolue constamment, et de nouvelles menaces apparaissent, ce qui rend encore plus important de mettre en place des mesures de sécurité rigoureuses et de former régulièrement les citoyens à l'importance de la protection de leurs données.

Il est essentiel de les informer régulièrement sur leurs droits et les actions qu'ils doivent entreprendre en cas de violation de leur confidentialité.

Le Maroc dispose d'un cadre juridique solide et pionnier en Afrique.

CNDP joue un rôle important, mais elle fait face à des défis en termes de ressources, de visibilité et d'efficacité.

Sa mise en œuvre dans le secteur public et privé reste inégale.

Des pistes positives se dessinent pour l'adoption de normes internationales de protection des données au Maroc, ainsi que pour le renforcement des moyens humains et techniques de la CNDP.

La désignation d'un DPO dans les organismes publics et les grandes entreprises est devenue obligatoire, tout en exigeant la généralisation des DPIA pour les traitements sensibles.

Par ailleurs, il est nécessaire de développer une culture de protection des données, notamment à travers l'éducation numérique, en encourageant l'adoption de normes techniques de sécurité obligatoires.

De plus, afin de renforcer davantage la protection des données personnelles, le Maroc doit accélérer son adhésion à la Convention 108+ du Conseil de l'Europe et travailler à obtenir une reconnaissance d'adéquation avec l'Union européenne.

Le modèle marocain, avec une loi avancée et une autorité spécifique, s'inspire du RGPD, mais reste marqué par des contraintes structurelles (indépendance, sanctions limitées).

Le modèle français (et plus largement européen) repose sur une autorité de contrôle indépendante, juridiquement forte, dotée de pouvoirs gradués et dissuasifs.

Le RGPD, entré en vigueur en 2018 en Europe, est un exemple pertinent, imposant des règles strictes pour collecter, utiliser, conserver et partager des données personnelles.

Il s'applique directement dans tous les pays membres, sans nécessiter une transposition nationale.

Ce règlement s'applique à toutes les organisations manipulant des données sur les citoyens européens, exigeant de la transparence, du consentement, de la sécurité, de la responsabilité et une notification en cas de violation.

Lorsqu'il y a un non respect, des sanctions sévères sont appliquées, ce qui souligne l'importance de ce cadre réglementaire pour les entreprises.

Le Québec adopte une modernisation progressive (Loi 25), avec des obligations strictes de gouvernance, la reconnaissance d'un droit civil (action privée) et des sanctions robustes, rapprochant ce modèle du RGPD tout en l'adaptant au contexte nord-américain.

En conclusion, il est important d'améliorer continuellement la protection des données en sensibilisant les citoyens, en renforçant les mesures de sécurité et en favorisant la collaboration entre les institutions chargées de la sécurité nationale et de la protection des données, ainsi qu'entre les pays.

Dans ce contexte, il convient de noter que les systèmes juridiques européens montrent diverses approches pour réglementer le traitement des données.

Cela est visible notamment en Bulgarie, en Espagne, en Pologne et au Portugal, où le Conseil supérieur de la magistrature veille au respect des normes de protection des données, soulignant l'adaptation des structures juridiques aux enjeux actuels.

Par conséquent, le Maroc, en tant que pays ambitieux sur le plan régional, s'inscrit dans une dynamique d'alignement international.

Il doit renforcer ses relations et collaborations avec ces pays, reconnus comme des leaders dans ce domaine, afin d'apprendre de leurs bonnes pratiques et de leurs cadres juridiques et institutionnels.

Néanmoins, conscients de la complexité de cette thématique et des débats qui s'engagent autour des politiques de protection des données personnelles, cette réflexion n'a pas la prétention d'avoir tout examiné.

Nous laissons donc le soin à d'autres chercheurs spécialistes du domaine d'apporter leurs précieuses contributions.

BIBLIOGRAPHIE

➢ **Ouvrages généraux:**

- Cassar B., (2020). La modernisation du service public de diffusion du droit, vers l'instauration d'une législation plateforme, Dalloz actualité.
- IFRAH L., (2010). L'Information et le renseignement par Internet. Que sais-je ?, n° 3881, PUF.

➢ **Ouvrages spéciaux:**

- 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 ?
- BANCK A., (2023). RGPD: la protection des données à caractère personnel, Ed.5, Editeur Gualino.
- MATTATIA F., (2021). RGPD ET DROIT DES DONNÉES PERSONNELLES. Enfin Un Manuel Complet Sur Le Nouveau Cadre Juridique Issu Du RGPD Et De La Loi, 5éme édition. Edition Eyrolles.

➢ **Thèses et mémoires :**

- HAOUNANI A. (2019). L'UTILISATION DES DONNEES PERSONNELLES DANS LE DROIT COMPARE, Mémoire pour l'obtention du Master Droit Du Numérique, soutenue en 2019. Faculté des sciences juridiques et politiques- université Hassan premier Settat/ Maroc.
- Vergnolle S. (2020). L'EFFECTIVITÉ DE LA PROTECTION DES PERSONNES PAR LE DROIT DES DONNEES A CARACTERE PERSONNEL. Thèse pour le doctorat en droit présentée et soutenue publiquement à l'université Paris II le 7 décembre 2020.

➢ **Articles :**

- HAOUNANI, .A. & AKKOUR, .S. (2023). LES DONNÉES PERSONNELLES À L'ÈRE DU BIG-DATA: QUEL CADRE JURIDIQUE AU MAROC ? Revue Internationale du chercheur. 4, 1.

➢ **Rapports:**

- PROTECTION DES DONNEES PERSONNELLES - ANALYSE COMPAREE DES LEGISLATIONS ET DES PRATIQUES /DANS NEUF PAYS EUROPEENS - dans le contexte du cadre juridique européen.
- Rapport sur la protection des données personnelles dans le cadre du secteur de la sécurité• au Maroc/ Séminaire. (2015). DCAF-CEDHD - Rabat, Maroc.
- Travaux de l'OCDE sur la vie privée. Dans: Organisation de coopération et de développement économiques [site Web]. (Paris, 2020).

➢ **Webographie:**

- Site officiel de la CNDP, consultable sur https://www.cndp.ma/fr/cndp/qui-sommes nous/commision.html
- Site officiel de la CNIL, consultable sur https://www.cnil.fr/fr/reglement-europeen protection-donnees
- Site officiel de la DGSSI, consultable sur https://www.dgssi.gov.ma/fr/presentation/dgssi/presentation-missions.html