Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 4, No. 4, Août 2026

La protection des données personnelles au Maroc à l'épreuve de l'effectivité juridique et institutionnelle

Nawal Es-shassah 1, Soumaya Akkour 2

1 Doctorante en droit du numérique à la faculté des Sciences Juridiques et Politiques, Université Hassan 1er de Settat.

ORCID: https://orcid.org/0009-0008-1977-8417

2 Professeure de l'Enseignement Supérieur à la faculté des Sciences Juridiques et Politiques, Université Hassan 1er de Settat.

ORCID: https://orcid.org/0009-0000-3860-1440

Abstract: Digitalization is now a major driver of global socio-economic development, and Morocco is fully part of this transformation. Accelerated after the pandemic, this process has contributed to modernizing public services, strengthening national competitiveness, and expanding electronic exchanges. However, this technological shift raises significant challenges, particularly regarding personal data protection and information systems security. To address these issues, Morocco has strengthened its legal framework through key legislation on personal data protection and cybersecurity. These rules aim to safeguard fundamental rights, regulate digital processing activities, support administrative digitalization, secure electronic transactions, and impose sanctions in cases of non-compliance with legal obligations.

Keywords: Companies; National Commission for the Protection of Personal Data (CNDP); Personal Data; Cyberattack; Automated Processing of Personal Data.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**21798595**

Résumé: La numérisation constitue aujourd'hui un levier majeur du développement socio-économique mondial, auquel le Maroc participe pleinement. Accéléré après la pandémie, ce processus a favorisé la modernisation des services publics, l'amélioration de la compétitivité nationale et l'essor des échanges électroniques. Toutefois, cette transformation soulève des risques liés à la protection des données personnelles et à la sécurité des systèmes d'information. Pour y répondre, le Maroc a renforcé son cadre juridique par des textes relatifs aux données personnelles et à la cybersécurité. Ces normes protègent les droits fondamentaux, encadrent les traitements numériques et prévoient des sanctions en cas de violation.

Mots clés: Les entreprises, la CNDP, les données personnelles, Cyberattaque, le traitement automatisé des données personnelles.

Introduction:

Dans le contexte mondialisé du XXIe siècle, la transformation numérique est devenue une priorité stratégique pour les pays cherchant à stimuler leur développement socio-économique et à renforcer leur position dans l'économie mondiale. Le Maroc, reconnu pour son engagement envers l'innovation et la modernisation, fait face à la pandémie de Covid-19, qui a révélé un cas d'étude particulièrement éclairant sur la manière dont la numérisation peut servir de catalyseur pour le progrès économique et social, ainsi que pour l'amélioration de la compétitivité internationale. L'avènement de la pandémie a renforcé l'urgence de considérer la numérisation comme un levier essentiel pour la transformation[1].

La numérisation touche tout autant la vie interne des organisations, les relations des marchés et les pratiques des individus que la façon de penser et de conceptualiser les phénomènes organisationnels et économiques. La capacité d'utiliser les TIC s'avère une composante importante dans la stratégie compétitive des entreprises, améliorer les mécanismes et les procédures de contrôle, acquérir une plus grande flexibilité et une moindre dépendance à l'égard du marché, développer des compétences stratégiques spécifiques et redéfinir les frontières de la concurrence. La vague de l'Internet et des TIC s'inscrit néanmoins dans une longue histoire de l'informatisation des organisations et des échanges[2].

Autrement dit, e monde numérique a considérablement transformé la manière dont les informations personnelles sont collectées, stockées et utilisées. Les entreprises, les gouvernements et d'autres organisations collectent et utilisent des quantités massives de données personnelles pour améliorer les produits et services, fournir une publicité ciblée et

[1] NEKHASS H., LAHIALA M.A., EL KORTBI I., YASSINE F.-E., ALAOUI FENNANE M.M., & LAHIALA A. (2024). LA NUMERISATION ET LE DEVELOPPEMENT SOCIO-ECONOMIQUE : CATALYSEUR DE COMPETITIVITE ET D'INNOVATION A L'ÈRE DU COVID-19 AU MAROC. Journal Des Sciences De l'Information Et De La Communication, 1(1), 146–154. https://doi.org/10.34874/PRSM.jsic-vol1iss1.930.

[2] BENGHOZI P.J., « L'économie Numérique : une économie disruptive », Cahiers français N° 392.

mieux comprendre les consommateurs. Cependant, cette collecte de données soulève des préoccupations en matière de vie privée et de protection des données[3].

Le droit des individus à la vie privée est donc impacté par le développement et l'expansion du gouvernement électronique, notamment par le droit à la confidentialité des informations. L'équilibre entre les avantages sociaux promis par le gouvernement électronique et les droits individuels à la confidentialité des informations est donc essentiel. Il est également crucial d'assurer une protection adéquate des données personnelles en gouvernant les systèmes d'information des organismes publics afin de renforcer la confiance du public envers l'administration en ligne, ce qui est crucial pour le succès de l'E-gouvernement[4].

Les entreprises ont un rôle primordial à jouer dans la préservation des données personnelles. Elles doivent se conformer à plusieurs obligations légales et réglementaires, telles que l'obtention du consentement des clients. Avoir des mesures de sécurité appropriées, restreindre la collecte et le traitement des informations personnelles, garantir le respect des droits des clients. La préservation des données personnelles représente un défi important pour les entreprises et les autorités publiques. Il est primordial de se conformer aux obligations légales en la matière afin d'éviter des sanctions significatives et de préserver la confiance des citoyens. De son côté, la cybersécurité met l'accent sur la préservation des systèmes informatiques, des réseaux et des données en ligne contre les risques et les attaques. Cela englobe des actions comme l'installation de pare-feu, la détection et la prévention des intrusions, la protection des données et la formation aux bonnes pratiques en matière de sécurité.

Dans cette situation, le gouvernement marocain a pris plusieurs lois, telles que la loi n° 09-08, la loi n° 05-20, la loi n° 07-03, la loi n°53-05 et la loi n°43-20, jouent un rôle essentiel. La mise en place de ces dernières était devenue indispensable afin de préserver la vie privée des utilisateurs d'internet[5]. De plus, de nombreuses législations concernant la préservation des données personnelles existent, comme le Règlement Général de la Protection des Données personnelles en Europe, ainsi que la convention 108... Aussi, afin de combattre l'utilisation abusive des données personnelles au Maroc, diverses institutions ont été mises en place afin de garantir la sécurité et la confidentialité des DCP.

Par ailleurs, l'essor du numérique au Maroc, à l'instar de la tendance mondiale, a profondément modifié les modalités de traitement des données personnelles, soulevant de nombreux enjeux liés à la vie privée, à la sécurité de l'information et à la souveraineté numérique. Dans ce contexte, la question de la protection des données personnelles ne relève plus uniquement du droit, mais s'impose comme un véritable enjeu sociétal, économique et technologique.

Dès lors, la problématique centrale de cet article s'articule autour de la question suivante : **Dans quelle mesure la loi 09-08 permet-elle d'assurer une protection effective des données personnelles au Maroc, et quels sont les principaux écarts entre le cadre juridique formel et les réalités institutionnelles et techniques de son application ?**

[3] AKKOUR S. & al. (2023), « PROTECTION DES DONNEES PERSONNELLES ET CYBERSECURITE », Revue Internationale du Chercheur « Volume 4 : Numéro 3 » p3.

[4] KOUNAIDI H., MAZOUZ Y., KOUNAIDI., « Impact de la loi 09-08 sur la gouvernance des systèmes d'information des administrations publiques marocaines » Revue du Contrôle de la Comptabilité et de l'Audit, Numéro 7 : Décembre 2018.

[5] AKKOUR S. & al. (2023) « PROTECTION DES DONNEES PERSONNELLES ET CYBERSECURITE », Revue Internationale du Chercheur « Volume 4 : Numéro 3»,op.cit, p3.

Cette interrogation vise à analyser, d'une part, la cohérence et la portée normative de la loi 09-08 au regard des standards internationaux, et d'autre part, à identifier les obstacles institutionnels, pratiques et culturels qui freinent son application sur le terrain. Elle s'inscrit dans une démarche à la fois juridique et empirique, combinant l'analyse du droit positif et l'étude des perceptions et pratiques des acteurs concernés.

1 : Le cadre normatif et institutionnel de la protection des données personnelles au Maroc

Dans un contexte de numérisation croissante, la préservation des informations personnelles constitue un enjeu majeur tant pour les États que pour les individus[6]. Conscient de cette importance, le Maroc a mis en place un cadre juridique et institutionnel robuste visant à garantir la confidentialité et la sécurité des données personnelles de ses citoyens.

1.1. Le cadre juridique de la protection des données personnelles

La protection des données à caractère personnel repose avant tout sur un socle juridique solide qui fixe les règles, principes et obligations applicables aux acteurs concernés. Nous allons étudier le cadre juridique marocain régissant la protection des données personnelles, en analysant les lois et règlements nationaux qui encadrent cette matière (1.1.1).

Par ailleurs, dans un contexte marqué par la mondialisation et la circulation transfrontalière des données, la protection des données ne saurait être pleinement effective sans la prise en compte des normes internationales. Ainsi les principaux instruments juridiques internationaux et les conventions auxquels le Maroc adhère ou s'inspire pour renforcer sa législation nationale (1.1.2). Et aussi fournir une compréhension claire des fondements juridiques qui garantissent la protection des données personnelles, en soulignant les interactions entre droit national et droit international.

1.1.1. Les textes internationaux en matière de la protection des données personnelles

La protection des données personnelles constitue un enjeu mondial qui dépasse les frontières nationales, surtout à l'ère de la globalisation numérique[7]. Le Maroc, en tant qu'acteur engagé sur la scène internationale, s'est aligné sur plusieurs normes et conventions internationales destinées à renforcer la protection de la vie privée et des données à caractère personnel.

L'objectif est de montrer que la protection des données personnelles est un enjeu universel, où les engagements internationaux viennent compléter et renforcer les dispositifs nationaux.

- **La convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel**

La croissance exponentielle des technologies de l'information, la préservation de la vie privée et des informations personnelles est devenue un enjeu majeur pour nos sociétés contemporaines. Internet s'est imposé comme un moyen indispensable de communication et d'échanges variés. Les réseaux sociaux et le commerce en ligne sont en plein essor, ce qui entraîne des dangers pour les données personnelles de leurs utilisateurs.

Les textes nationaux et internationaux reconnaissent la notion de vie privée, et plus spécifiquement le droit à la protection des données personnelles, ainsi que les politiques mises en œuvre par les sites Web. Il est généralement reconnu que toute information qui permet

[6] LUCAS A., DEVESE J., FRAYSSINET J., Droit de l'informatique et de l'internet, Edition PUF, Paris, 2001. p.9.

[7] DARIUSZ K. & DE HERT P., "*Data protection as a human right", in Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. & Nouwt, S. (Eds.), Reinventing Data Protection ?* , Springer, 2009, pp. 77– 99.

d'identifier une personne peut compromettre sa vie privée, telles que son nom, prénom, numéro de téléphone, carte bancaire, sécurité sociale, ainsi que ses adresses électroniques et internet[8].
Tous les grands textes internationaux accordent une grande importance à la protection de la vie privée, comme l'affirme l'article 8 de la Convention européenne des droits de l'homme qui affirme le droit au respect de la vie privée[9].
Tout d'abord, il convient de signaler que la Convention 108 du Conseil de l'Europe constitue un texte fondateur contraignant tendant à protéger les personnes contre l'usage abusif du traitement automatisé des DCP[10], et à réglementer les flux transfrontaliers des données. Elle a été signée à Strasbourg le 28 janvier 1981, et porte sur la protection des personnes à l'égard du traitement automatisé des données.
A cet égard, ladite Convention crée une zone d'échange protégée entre les États l'ayant ratifié afin de respecter les principes communs permettant un niveau de protection équivalent. Cependant, il est à signaler que la Convention a laissé le soin au législateur interne d'adopter les mesures nécessaires à son application, ce qui ne lui donne pas d'effet direct en droit interne[11].

- **La convention de Malabo sur la cybersécurité et la protection des DCP**

Au fil des dix dernières années, l'Afrique a fait d'importants progrès dans la construction des infrastructures nécessaires aux TIC et a développé une connexion de plus en plus étroite. C'est pourquoi il était essentiel d'assurer la sécurité dans cet espace, qui est sujet à de nombreuses menaces. C'est pourquoi les chefs d'État et de Gouvernement, conscients des dangers causés par le phénomène de la cybercriminalité, se sont réunis les 26 et 27 juin 2014 à Malabo lors de la 23e session ordinaire du Sommet de l'UA pour adopter la Convention africaine sur la cybersécurité et la protection des DCP.
A cet égard, il est à noter qu'en 2016, le Sénégal en est devenu Etat partie, après le Maroc et l'Ile Maurice[12]. Ce texte était très attendu par les acteurs du Numérique en Afrique et dans le monde. Ainsi, il constitue une innovation majeure de la stratégie de lutte contre la cybercriminalité en Afrique en visant à créer un cadre normatif approprié correspondant à l'environnement numérique[13].
A ce titre, on note que la Convention de Malabo présente la particularité d'intégrer l'approche de cybersécurité dans la stratégie de lutte, impliquant notamment la promotion de la culture de la cybersécurité, l'élaboration d'une politique nationale, la sensibilisation des populations, la

[8] CHASSIGNEUX C., « La protection des données personnelles en France », (2001) Vol 6-Numéro2 Lex Electronica.
[9] Art 8 Al 1 de la CEDH prévoit que « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».
[10] Salle de presse Convention 108+ : la nouvelle version d'un instrument phare, publié au Portail du CONSEIL DE L'EUROPE, le 18 Mai 2018, cité par, https://www.coe.int/fr/web/data-protection/-/modernisation-of-convention 108
[11] FENOLL-TROUSSEAU M.P., HAAS G., « Internet et protection des données personnelles » , Paris Editions ,Litec , 2000 , p39.
[12] QUEMENER M., « Le droit face à la disruption numérique, adaptation des droits classiques, émergence de nouveaux droits » p.186.
[13] BADIL M., « Dispositif juridique et institutionnel en matière de lutte contre la cybercriminalité au Maroc Défis et perspectives- », Approches-Fès, 1ère édition 2022, p 60.

formation des acteurs et la mise en place de structures dédiées (CERT[14], structure d'investigation, …).

On note que l'option de la ratification de la Convention de Malabo et de l'adhésion à la Convention européenne de Budapest révèle au grand jour que les autorités ont pris conscience des enjeux stratégiques qui s'attachent à la diversification des mécanismes de coopération en matière de cybersécurité et de cybercriminalité[15].

- **Le règlement général sur la protection des données**

Le RGPD est une législation européenne indispensable qui renforce et consolide les droits et la protection des données personnelles des individus. L'entrée en vigueur de ce nouveau règlement européen le 25 mai 2018 concerne les traitements de données personnelles, qu'ils soient effectués sur des supports informatiques (logiciels, sites web...), mais aussi sur des supports papier, L'application du RGPD concerne toutes les associations, peu importe leur taille, leur structure et leur secteur d'activité.

En ce qui concerne le RGPD, il a pour objectif d'accompagner le développement exponentiel de la science et des technologies en unifiant et renforçant la protection des droits de propriété intellectuelle en Europe. Dans cette optique, en plus des droits classiques (information, accès, rectification, opposition, restriction du profilage automatisé utilisé pour prendre une décision, etc.), le RGPD a ajouté de nouveaux droits aux individus, tels que le renforcement des conditions relatives au consentement, en particulier celui des enfants, le droit à l'oubli, le droit à la limitation du traitement et le droit à la portabilité des données. De la même manière, le nouveau Règlement communautaire encouragera une augmentation du pouvoir de sanction, qui pourra maintenant atteindre 4% du chiffre d'affaires annuel et mondial du contrevenant[16].

Dans cette optique, une section consacrée au RGPD a été ajoutée en mai 2017 sur le site Internet de la CNDP pour faciliter l'acquisition du nouveau règlement par les entreprises concernées. D'autres mesures d'accompagnement identifiées en collaboration avec les départements ministériels et les fédérations professionnelles concernées seront mises en place dans les mois à venir[17].

1.1.2 Le cadre juridique Marocain de la protection des données personnelles

L'environnement légal marocain en matière de protection des données personnelles repose sur un ensemble de textes législatifs essentiels, conçus pour répondre aux enjeux liés à la numérisation et à la gestion des informations sensibles. L'adoption de la loi n° 09-08 en 2009 a posé les fondations de la protection des données personnelles au Maroc, en instaurant des règles strictes concernant la collecte, le traitement et la conservation des informations à caractère personnel.

[14] Computer Emergency Response Team : signifie dans le secteur de la sécurité des organismes certifiés et indépendants, assurant des services d'alerte, de prévention des risques et d'assistance au traitement d'incidents suite à des attaques informatiques.

[15] QUEMENER M., « Le droit face à la disruption numérique, adaptation des droits classiques, émergence de nouveaux droits », Gualino éditeur, lextenso éditions, 2018, p 186.

[16] ITEANU O., « Quand le digital défie l'Etat de Droit », Editions EYROLLES, Paris,2016, p 71.

[17] HANDAOUI K., « La CNDP apelle les entreprises à se conformer au règlement européen », cité par, BADIL M., « Dispositif juridique et institutionnel en matière de lutte contre la cybercriminalité au Maroc -Défis et perspectives » ,op.cit,p 64.

La loi n° 07-03 vient compléter ce dispositif en assurant la protection des individus contre les traitements illégaux des données dans des secteurs sensibles tels que la sécurité nationale et la défense. Plus récemment, la loi n° 05-20 a renforcé ce cadre en régulant l'usage des technologies numériques, notamment dans le domaine de la cybersécurité, afin de répondre aux défis croissants posés par les innovations technologiques.

- **La loi 09-08 relative à la Protection des Personnes Physiques à l'Egard du Traitement des Données à Caractère Personnel[18]**

La loi 09-08 concernant la protection des données personnelles a pour objectif de garantir la protection des droits des individus en ce qui concerne l'utilisation de leurs informations personnelles. En d'autres termes, cette loi inclut un ensemble de mesures légales visant à garantir la protection des données physiques contre les traitements de leurs données personnelles au Maroc. La CNDP a également été fondée par elle, l'adoption de cette loi fait partie de la dynamique internationale visant à encourager le droit à la protection de la vie privée et à renforcer la confiance numérique dans notre pays. D'une part, et aussi pour promouvoir le plan national de L'État marocain concernant le E-gouvernement et le Maroc numérique.

Le Maroc a adopté la loi 09-08 afin de favoriser le développement du secteur tertiaire, en autorisant la migration d'activités du secteur en provenance d'Europe. Selon les lois en vigueur, il est requis que les informations personnelles soient collectées et traitées avec responsabilité et en respectant les droits fondamentaux de l'individu[19].

Le législateur marocain a d'abord établi plusieurs termes concernant le traitement des DCP. L'article 1er de la loi 09-08 [20]stipule, entre autres, que les DCP englobent toute information, peu importe sa nature et indépendamment de son support, ce qui signifie que les DCP présentées sur support numérique sont conclues.

Dans le cadre de la protection garantie par le législateur marocain, la loi en question requiert d'abord le consentement[21] libre, clair et incontestable de la personne concernée pour le traitement de ses données.

Il est essentiel de traiter les données à caractère personnel de manière honnête et légale, et de les recueillir dans des buts clairement définis, explicites et légitimes. Il est important qu'elles ne soient pas utilisées de manière incompatible avec ces objectifs.

Mais s'il y a un intérêt légitime et si le responsable du traitement en fait la demande, la Commission nationale peut permettre la conservation des données à des fins historiques, statistiques ou scientifiques au-delà de cette période. Le responsable du traitement est enfin chargé de s'assurer du respect de ces dispositions, sous l'autorité de la Commission nationale[22].

[18] Dahir n°1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, B.O 5711 du 23 février 2009, p552.

[19] 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» p 438.

[20] Al 1er de l'article 1er de la loi 09-08 prévoit : « données à caractère personnel »: toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable, dénommée ci-après « personne concernée ».

[21] Al 9, Art 1 de la loi 09-08 stipule que « consentement de la personne concernée » : toute manifestation de volonté, Libre, spécifique et informée, par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement ».

[22] Art 3 de La loi 09-08 relative à la Protection des Personnes Physiques à l'Egard du Traitement des

- **La loi 05-20 relative à la cybersécurité**

Face à l'évolution des risques de cybercriminalité à l'échelle mondiale, le Maroc s'est bâti au cours de ces dernières années un arsenal juridique relatif à la cybersécurité et à la protection de données englobant notamment : la loi 07.03 en 2003, la loi 09.08 en 2009 et la dernière en date, la loi 05.20[23] relative à la cybersécurité dont le projet a été adopté par la chambre des représentants le 06 juillet 2020, Est entrée en vigueur au Maroc dès le 30 Juillet 2020.

La loi 05-20 relative à la cybersécurité[24] vise à consolider la confiance numérique, à favoriser la digitalisation de l'économie et à garantir la continuité des activités économiques et sociétales du Maroc. Elle s'inscrit dans le cadre de la Stratégie Nationale de Cybersécurité, dont l'un des principaux objectifs est la protection et la résilience des systèmes d'information des entités publiques, notamment les administrations, les collectivités territoriales, les entreprises publiques et les infrastructures d'importance vitale (IIV)[25].

La loi impose aux entités[26] des règles minimales de sécurité pour assurer la fiabilité et la résilience de leurs systèmes d'information. Ces règles incluent des mesures techniques et organisationnelles pour gérer les risques cybernétiques et prévenir les incidents. Il est obligatoire pour les entités de faire part de tout incident de sécurité à l'Autorité nationale de cybersécurité, de nommer un responsable de la sécurité et de mettre en œuvre des plans de continuité afin de réagir rapidement en cas de crise.

- **La loi 07-03 relative aux STAD**

Le Maroc à renforcer son arsenal juridique au niveau des systèmes de traitement automatisé des données par la loi n° 07-03, cette dernière constitue une étape décisive pour le Royaume. Il ne s'agit pas d'un texte s'appliquant uniquement à des cas bien définis mais d'une loi complétant le code pénal, elle couvre de nombreux agissements frauduleux imputables à l'informatique. Les principales accusations formulées dans cette loi portent sur les intrusions et les violations des systèmes de traitement automatisé des données.

Le législateur Marocain a adopté une approche proactive en adoptant la loi 07- 03[27]relative aux atteintes liées aux systèmes de traitement automatisé des données. Cette loi a été intégrée dans le code pénal marocain, aux articles 607-3 à 607-11.

Reproduite à partir de la loi française du 5 janvier 1988 dite loi Godfrain, la loi N° 07-03 constitue un texte fondateur pour la mise à niveau de l'arsenal juridique marocain afin de tenir

Données à Caractère Personnel.

[23] TAHORI L., « La protection de l'employé à la lumière de la loi 09-08 », disponible sur le lien suivant : https://revuealmanara.com/la-protection-de-lemploye-a-la-lumiere-de-la-loi-09-08

[24] NOTE DE PRESENTATION RELATIVE A LA LOI N° 05-20 SUR LA CYBERSECURITE, disponible sur https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/,p2

[25] Les Infrastructures d'Importance Vitale (IIV) » : sont des installations ou services essentiels au fonctionnement et à la sécurité d'un pays. Elles englobent des secteurs clés comme l'énergie, les télécommunications, les transports, la santé et les finances. Toute perturbation de ces infrastructures pourrait avoir des conséquences graves sur la société, l'économie ou la sécurité nationale.

[26] Selon art 3 de la loi 05-20 « Chaque entité doit veiller à ce que ses systèmes d'information soient conformes aux directives, règles, règlements, référentiels ou recommandations, édictés par l'autorité nationale ». De même , l'alinéa 1er de l'art 4 de la loi 05-20 dispose « Chaque entité doit élaborer et mettre en œuvre une politique de sécurité de ses systèmes d'information qui soit conforme aux directives de l'autorité nationale ».

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

compte des infractions imputables à la criminalité numérique. Il existe, cependant, une distinction entre l'accès et le maintien frauduleux dans un STAD, et ce conformément aux dispositions de ladite loi. Cette loi traite les atteintes aux systèmes de traitement automatise des données (STAD) et réprime pénalement de nombreux comportements[28].

1.2. L'architecture institutionnelle de protection des données au Maroc

La mise en œuvre effective des lois relatives à la protection des données personnelles au Maroc repose sur un cadre institutionnel structuré, chargé de veiller au respect des principes juridiques énoncés. Ce dispositif institutionnel vise non seulement à encadrer les pratiques en matière de traitement des données, mais également à promouvoir une culture de respect de la vie privée dans un environnement numérique en constante évolution.

1.2.1 La Commission nationale de contrôle de la protection des Données à caractère Personnel (CNDP)

Elle est un organisme spécialisé, créé par la loi 09-08 sur la protection des personnes contre le traitement des données à caractère personnel, afin de garantir la mise en œuvre des droits et des responsabilités établis par cette loi.

Cette Commission a donc pour mission de vérifier la légalité du traitement et de superviser l'application de la législation en vigueur, afin de préserver la vie privée et de protéger les libertés et droits fondamentaux de l'homme contre toute atteinte numérique. Dans cette optique, la CNDP s'efforce de trouver un juste équilibre entre l'utilisation des DCP et le respect des droits des personnes concernées.

Il est à noter que cette institution a fait du Maroc un des États pionniers en matière de protection des DCP dans le monde arabe et musulman, vu qu'elle s'inscrit parfaitement dans le cadre de l'article 24 de la constitution de 2011[29]qui consacre le droit de chaque personne à la protection de sa vie privée[30].

La mise en place de la CNDP marque une avancée majeure dans l'intégration du Maroc dans l'économie et la société numérique à l'échelle nationale et internationale. Cette institution vise à renforcer et renforcer son statut interne, tout en étant autorisée à participer, auprès de l'autorité gouvernementale compétente, aux négociations internationales en la matière, conformément à la loi 09-08[31]. Ainsi, La Commission a donc mis en place des actions au sein de l'Association francophone des Autorités de Protection des Données Personnelles (AFAPDP) dans le cadre de cette visibilité internationale.

1.2.2 Autres institutions en charge de la protection des données personnelles

Au Maroc, divers organismes occupent une place centrale dans la préservation des informations personnelles et la sécurité des systèmes d'information. Ces entités ont pour mission d'assurer la confidentialité des données, de combattre les Cybermenaces et de contrôler l'utilisation des

[28] ENNASHI K., « la criminalité numérique droit marocain » , 1 ère édition 2020 , p25.

[29] L'article 24 de la Constitution de 2011 prévoit que : « Toute personne a droit à la protection de sa vie privée. (...) Les communications privées, sous quelque forme que ce soit, sont secrètes (…) ».

[30] Art 1 de la loi 09-08 dispose que : « L'information est au service du citoyen (...). Elle ne doit pas porter atteinte à l'identité, aux- droits et libertés collectives ou individuelles de l'homme. Elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens ».

[31] Rapport d'activité de la CNDP, 2010-2013, sur https://www.cndp.ma/wp-content/uploads/2023/01/Rapport-activite-CNDP-2010-2013-fr.pdf ,op.cit , p 13.

informations personnelles. Dans cette optique, le Maroc a mis en place une série d'organismes de cybersécurité, on peut mentionner :

- **La Direction Générale de la Sûreté Nationale (DGSN)**

La police nationale du Maroc est dirigée par la DGSN, Fondée le 16 mai 1956 par le Roi Mohammed V, elle a été créée. Selon le dahir n° 1-56-115 du 5 chaoual 1373 (16 mai 1956), la DGSN est soumise à des règles[32]. Rattachée au Ministère de l'Intérieur et dirigée par un directeur générale nommé par Dahir royal, la DGSN agit dans les communes urbaines et travaille en collaboration avec la Gendarmerie royale marocaine. Ses attributions sont définies par le décret du 7 Avril 2010[33].

Dès lors, toutes ces missions doivent se faire dans le respect des libertés individuelles et collectives telles que garanties par la constitution de 2011[34]. Soucieuse de lutter efficacement contre toute forme de criminalité, notamment la criminalité organisée et transnationale, la DGSN accorde une importance privilégiée à la coopération internationale en participant aux conférences régionales, intercontinentales et internationales en vue de renforcer les liens de coopération entre le Maroc et les autres pays dans le domaine de sécurité et d'échange des expériences et des informations en matière de lutte contre la criminalité internationale, sous toutes ses formes, et en œuvrant constamment pour la redynamisation des différents canaux dont elle dispose.

Dans ce cadre, plusieurs enquêtes ont été menées par la DGSN concernant des opérations internationales de cybercriminalité avec les services de pays étrangers, comme le FBI. A ce titre, le partage d'informations se fait aussi avec les pays Interpol coopérant dans les affaires de cybercrime. Parmi ces pays, figurent l'Allemagne, la Belgique, le Canada, les États-Unis, Hong-Kong, Chine, Monaco, France, Royaume Uni…

- **Le Comité Stratégique de la cybersécurité (CSC)[35]**

Créé par la loi n° 05-20 du 25 juillet 2020, le Comité Stratégique de la cybersécurité (CSC), anciennement appelé le Comité Stratégique de la Sécurité des Systèmes d'Information, est l'organisme responsable de définir les orientations stratégiques de l'État en matière de cybersécurité. La création du CSSSI fut décidée par le Décret n° 2-11-508 du 21 septembre 2011. La mise en place de ce Comité fait partie d'une stratégie militaire et sécuritaire plus large, qui vise à renforcer les capacités nationales en matière de sécurité numérique.

Conformément aux dispositions de l'article 2 du décret n° 2-21-406, le comité stratégique de la cybersécurité est présidé par le ministre délégué auprès du chef du gouvernement chargé de l'administration de la défense nationale. Il se compose de plusieurs membres.[36]

[32] Publiée au B.O n 2274 du 25/05/1956, p 46.

[33] Décret n°2.10.84 du 21 Rabia II 1431(7 avril 2010), publié le 26 Rabia II 1431 (12 Avril 2010) relatif aux attributions de la Direction Générale de la Sûreté Nationale, B.O n°5829, du 07/04/2010, p 2462.

[34]Interpol, CONNECTING POLICE FOR A SAFER WORLD https://www.interpol.int/fr/Pays-membres/Afrique/Maroc.

[35] Direction générale de la sécurité des systèmes d'information (DGSSI), « Comité stratégique de la cybersécurité », Rabat, Administration de la Défense nationale, consulté le 11 juin 2026.

[36] Site officiel de la DGSSI : https://www.dgssi.gov.ma/fr/comite-strategique-de-la-cybersecurite

Il est chargé en outre de[37]: Veiller sur la résilience des SI des entités, des infrastructures d'importance vitale et des opérateurs177 visés à la section III du chapitre II de la loi n° 05-20, évaluer annuellement le bilan d'activité de la direction générale de la sécurité des systèmes d'information, évaluer les travaux du comité national de gestion des crises et évènements cybernétiques majeurs prévu à l'article 36 de la loi susmentionnée n° 05-20……

- **La Direction de la Sécurité des systèmes d'Information (DGSSI)**

La DGSSI a été créée par Décret n° 2-11-509 du 21 septembre 2011. Elle est rattachée à l'Administration de la Défense Nationale du Royaume du Maroc. Elle joue un rôle crucial dans la préservation et la sécurisation des systèmes d'information de l'État. Elle est responsable de la coordination des efforts interministériels visant à élaborer et mettre en place la stratégie nationale de sécurité des systèmes d'information, tout en assurant l'application des directives et des orientations établies par le comité stratégique en ce domaine.

Elle est un système de surveillance, de détection et d'alerte des événements pouvant compromettre la sécurité des systèmes d'information de l'État et coordonne les mesures à prendre en conséquence. Elle se focalise aussi sur la formation et la sensibilisation du personnel des administrations et des organismes publics, tout en assurant la gestion des autorisations et des déclarations concernant les moyens de cryptographie.

De plus, elle effectue également une surveillance technologique pour prévoir les changements et proposer des avancées en matière de sécurité des systèmes d'information. Finalement, elle propose un soutien et des recommandations aux administrations, aux organismes publics et au secteur privé afin de garantir la sécurité de leurs systèmes d'information, tout en mettant en place les outils techniques requis à cet effet.[38]

- **Le Centre Marocain d'Alerte et de Gestion des Incidents Informatiques (MA-CERT)**

La stratégie nationale pour la société de l'information et de l'économie numérique a inscrit la problématique de la confiance numérique parmi ses thèmes prioritaires. Pour ce faire, le projet « Ma-CERT » (Moroccan Computer Emergency Response Team) relatif à la création du Centre Marocain d'alerte et de gestion des incidents informatiques a été lancé, le lundi 17 janvier 2011 au siège principal du ministère Marocain de l'industrie du commerce et des nouvelles technologies, par l'Agence coréenne de coopération internationale (KOICA). Ce projet s'inscrivait dans le cadre du programme « Maroc Numérique 2013 »[39].

La Direction de gestion de ce centre, l'une des quatre directions de la DGSSI, a pour mission de mettre en place, en collaboration avec les autres administrations, des systèmes de surveillance, de détection et d'alerte des événements pouvant compromettre la sécurité des systèmes d'information de l'État et de coordonner la réaction à ces événements.

Le ma-CERT a été mis en place dans le but de renforcer la sécurité des systèmes d'information, avec pour objectifs : disponibilité, intégrité, confidentialité et traçabilité. En effet, dans le cadre des actions visant à renforcer la SSI des administrations et organismes publiques et

[37] « Les administrations de l'Etat, les collectivités territoriales, les établissements et entreprises publics et toute autre personne morale de droit public ».

[38] Site officiel de la DGSSI : https://www.dgssi.gov.ma/fr/dgssi

[39] BADIL M., « Dispositif juridique et institutionnel en matière de lutte contre la cybercriminalité au Maroc - Défis et perspectives-», éd. Approches-Fès, 2022,op.cit,p 195.

infrastructures d'importances vitales, le Centre de veille de détection et réaction aux attaques informatiques (ma-CERT) propose un service d'assistance à la réponse aux incidents de cybersécurité

Il est important de souligner que le centre n'a pas encore mis en place une plateforme de signalement qui permettra aux internautes marocains de signaler les sites illicites tels que les sites pédopornographiques, les sites incitant à la haine et aux injures raciales, au terrorisme, ainsi que de déclarer les incidents de cybercriminalité, comme cela se fait par exemple actuellement en France[40].

2. L'effectivité de la protection des données personnelles au Maroc

2.1. Une démarche pratique fondée sur l'analyse de cas réels

Afin d'apprécier l'effectivité de la protection des données personnelles au Maroc, la présente étude substitue à la démarche qualitative par entretiens une analyse fondée sur des cas réels, marocains et internationaux. Cette orientation permet de confronter le cadre normatif, notamment la loi n°09-08, aux situations concrètes dans lesquelles les autorités de régulation sont intervenues pour contrôler, encadrer ou sanctionner les pratiques de traitement des données personnelles[41].

2.1.1. La démarche méthodologique adoptée

L'analyse est construite autour de cas sélectionnés en raison de leur pertinence juridique et pratique. Au Maroc, l'opération de contrôle menée par la CNDP sur les sites web constitue un premier indicateur de l'application concrète de la loi n°09-08[42], notamment en matière d'information des personnes concernées, de notification des traitements, de proportionnalité et d'usage des cookies. De même, l'affaire relative au transfert non notifié d'images issues de dispositifs de vidéosurveillance vers des institutions situées à l'étranger illustre les enjeux liés aux flux transfrontaliers de données et au contrôle exercé par la CNDP sur les responsables de traitement.

L'intervention de la CNDP à l'égard de Facebook permet également d'observer les difficultés posées par les grandes plateformes numériques étrangères, notamment concernant le traitement des plaintes, la localisation des données, le droit à l'oubli, la géolocalisation et le profilage des utilisateurs marocains. Cette affaire révèle que l'effectivité du droit national dépend non seulement de l'existence d'obligations légales, mais aussi de la capacité de l'autorité nationale à dialoguer avec des opérateurs numériques transnationaux.

Sur le plan comparatif, l'affaire Google Analytics traitée par la CNIL[43] en France montre que les outils numériques courants peuvent soulever des difficultés sérieuses en matière de transfert international des données. L'arrêt Meta Platforms c. Bundeskartellamt[44] rendu par la Cour de

[40] EL AZZOUZI A., « La Cybercriminalité au Maroc », BISHOPS SOLUTION , 2022 ,op.cit,p 143.

[41] Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), « Infraction à la loi 09-08 suite à absence de notification à la CNDP », communiqué de presse, Rabat, 9 janvier 2023.

[42] Royaume du Maroc, loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, promulguée par le dahir n°1-09-15 du 18 février 2009.

[43] Commission nationale de l'informatique et des libertés (CNIL), « Utilisation de Google Analytics et transferts de données vers les États-Unis : la CNIL met en demeure un gestionnaire de site web », lettre d'information, février 2022.

[44] Cour de justice de l'Union européenne, grande chambre, 4 juillet 2023, Meta Platforms Inc. e.a. c. Bundeskartellamt, aff. C-252/21, ECLI:EU:C:2023:537.

justice de l'Union européenne illustre, quant à lui, l'articulation croissante entre la protection des données personnelles et le droit de la concurrence, en particulier lorsque l'exploitation des données renforce le pouvoir économique d'une plateforme dominante.

2.1.2 Analyse croisée de la responsabilité des acteurs publics et privés dans la protection des données personnelles

La Loi n°09-08, adoptée en 2009, a longtemps constitué une avancée pionnière dans l'espace juridique marocain en matière de protection des données à caractère personnel. Toutefois, près de deux décennies plus tard, cette loi semble désormais dépassée face à l'ampleur des mutations technologiques et aux nouveaux usages du numérique.

Or, la Loi 09-08, conçue à une époque où ces innovations n'étaient encore qu'embryonnaires, ne prévoit ni des définitions précises, ni des mécanismes adaptés pour encadrer ces usages. Elle demeure ainsi trop générale, parfois lacunaire, et insuffisamment contraignante pour répondre aux risques accrus que ces évolutions technologiques font peser sur les droits des personnes.

Face à ce constat, une réforme d'ampleur du cadre juridique s'impose. C'est dans cette perspective qu'a été déposée, à la Chambre des représentants, la proposition de loi n°272/2023[45], qui vise à moderniser en profondeur le dispositif national. Inspirée des standards internationaux, en particulier du Règlement général sur la protection des données (RGPD) de l'Union européenne, cette réforme ambitionne d'aligner le Maroc sur les meilleures pratiques internationales en matière de gouvernance des données.

Parmi les principales innovations, figure la transformation de la CNDP en « Instance Nationale » (الهيئة الوطنية), dotée d'une personnalité morale et d'une autonomie administrative et financière renforcées. Cette mutation structurelle vise à doter l'autorité de contrôle d'une indépendance effective, gage de crédibilité et de légitimité dans l'exercice de ses missions. La gouvernance serait désormais assurée par une structure tripartite (Conseil, Président, Directeur Général), avec une composition mixte intégrant des nominations parlementaires et royales, renforçant ainsi la légitimité démocratique de l'institution.

2.2. Les défis liés de la protection des données personnelles au Maroc

La préservation de la confidentialité, de l'intégrité et de la sécurité des données à caractère personnel constitue aujourd'hui un enjeu fondamental, tant pour les institutions publiques que pour les opérateurs privés. Toutefois, la mise en œuvre effective de ce droit demeure insuffisante et se heurte à une série d'obstacles complexes, appelés à évoluer constamment dans un contexte numérique globalisé.

Ces défis sont pluriels : technologiques, en raison de la rapidité des innovations et de la sophistication croissante des cyberattaques ; juridiques, du fait de l'écart souvent constaté entre les textes législatifs et les réalités pratiques ; institutionnels, en raison des limites structurelles et opérationnelles des organes de régulation ; et éthiques, face aux tensions croissantes entre progrès technologique et respect de la vie privée[46].

[45] Proposition de loi n°272/2023 modifiant et complétant la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, déposée à la Chambre des représentants le 21 juillet 2023.

[46] BOULAFDOUR B., La gouvernance des systèmes d'information au Maroc : une étude empirique, Revue du Contrôle de la Comptabilité et de l'Audit, Numéro 6 : Septembre 2018.

2.2.1 Les défis juridiques et institutionnel liés de la protection des données personnelles au Maroc

Malgré l'adoption de la loi 09-08 et la mise en place d'un cadre institutionnel dédié, des obstacles persistants entravent l'effectivité de la protection des données personnelles au Maroc. Cette section propose une analyse des limites d'ordre juridique et institutionnel.

- **Les défis juridiques**

Comme évoqué précédemment, le Maroc a adopté une loi sur la protection des données personnelles dans le but de mettre en conformité sa législation nationale avec ses engagements internationaux. Si les participants du séminaire ont salué cette initiative, ils ont néanmoins plaidé en faveur d'un renforcement de la loi 09-08, notamment en matière de sanctions et d'indépendance administrative et financière de la CNDP. Certains participants regrettent également que la loi 09-08 ne prévoie pas de mécanismes de participation de la société civile à travers le CNDH.

Par ailleurs et d'après certains intervenants et afin de prévenir la collecte et le traitement abusifs de données à caractère par les autorités publiques ou des entités privées, il est nécessaire que la réglementation soit étendue à d'autres types de fichiers. Par exemple, l'intervention du législateur parait nécessaire pour combler le vide en matière de biométrie, de surveillance et de géo-localisation.

L'absence de réglementation spécifique pour l'IA au Maroc peut également dissuader les investissements dans ce secteur, car les investisseurs pourraient être incertains quant à la manière dont les données seront utilisées et protégées. En mettant en place des réglementations claires, le Maroc peut garantir la protection des droits fondamentaux des citoyens, tout en encourageant le développement économique dans ce secteur en pleine croissance[47].

- **Les défis institutionnels**

Plusieurs participants au séminaire ont souligné la nécessité de renforcer la bonne gouvernance au sein des institutions, notamment de la CNDP. Tout d'abord, l'Instance devrait disposer de ressources financières et humaines suffisantes. La Commission dispose à ce jour de sept membres, mais cet effectif semble trop faible face à la charge de travail.

Certains participants ont aussi exprimé leur souhait de voir la CNDP plus transparente et ouverte envers les citoyens. En effet, si cette dernière dispose d'une stratégie de sensibilisation Les : rubriques radiodiffusées, conventions signées avec certains secteurs), ses activités de communication externe ont été insuffisantes en raison du manque de ressources humaines et financières auquel elle fait face. Il s'agit donc de remédier à ces manques afin de renforcer la visibilité de la CNDP. Les citoyens devraient par exemple mieux comprendre le cadre dans lequel elle opère (champ d'application de la loi) et la procédure pour recourir à ses services (déposer une plainte, demander un conseil….[48]

2.2.2 Les Défis techniques liés de la protection des données personnelles au Maroc

À l'ère du numérique, les avancées technologiques rapides dans les technologies de l'information et de la communication (TIC) représentent à la fois une opportunité et un défi

[47] AKKOUR S., HAOUNANI A. et ASSADI F., LA PROTECTION DES DONNÉES PERSONNELLES FACE À L'INTELLIGENCE ARTIFICIELLE, Revue Internationale du Chercheur, vol 4, n° 3, 2023, p 17.

[48] LAGTATI K. et EL HAMEL D., La protection des données personnelles au Maroc à l'ère du numérique, Revue Internationale Burak Des Etudes Juridiques Et Economiques, vol 1, NO 1, 2025, p 244.

majeur pour la protection des données personnelles. Cette section explore les difficultés techniques auxquelles le Maroc est confronté pour garantir la sécurité et la confidentialité des données à caractère personnel dans un environnement en constante évolution.

Elle met en lumière deux aspects essentiels : d'une part, l'adaptation nécessaire aux innovations technologiques telles que l'intelligence artificielle, l'Internet des objets (IoT) ou la blockchain, qui bouleversent les modes traditionnels de collecte et de traitement des données ; d'autre part, la sécurisation des données face à la multiplication et à la sophistication croissante des cyberattaques, qui exigent la mise en place de systèmes robustes et une vigilance permanente.

- **L'adaptation aux nouvelles technologies**

L'évolution rapide des technologies de l'information et de la communication (TIC) pose des défis constants pour la réglementation. Les technologies émergentes, telles que l'intelligence artificielle, l'Internet des objets (IoT) et la blockchain, nécessitent une adaptation continue des cadres juridiques et des mesures de protection. L'utilisation massive des données grâce au Big Data et à l'Internet des objets promet de révolutionner le monde.

Les données à caractère personnel, sous diverses formes telles que les identifiants, les données de localisation, les préférences de consommation, les informations sur les achats, les recherches sur internet, les données de santé, les goûts et préférences, ainsi que les données financières, constituent un trésor précieux pour les entreprises. Elles permettent d'élaborer des stratégies de marketing ciblé en identifiant les besoins et intérêts spécifiques des consommateurs. La personnalisation des offres de produits et de services devient ainsi plus efficace, car les entreprises peuvent adapter leurs propositions en fonction des préférences individuelles des clients.

- **La sécurisation des données et la lutte contre les cyberattaques**

La difficulté majeure réside dans l'explosion exponentielle du volume de données générées et stockées. En 2025, le monde numérique compte plusieurs centaines de zettaoctets d'informations, dont une grande partie est sensible, qu'il s'agisse de données personnelles, financières ou industrielles. Cette masse colossale de données multiplie les points d'entrée potentiels pour les cyberattaques, rendant leur protection complexe et exigeant des solutions évolutives capables de gérer efficacement ces flux massifs.

Un autre défi crucial est la sophistication croissante des cyberattaques, notamment grâce à l'utilisation de l'intelligence artificielle par les hackers. Ces technologies permettent de concevoir des attaques plus furtives et adaptatives, capables de contourner les systèmes traditionnels de détection. Par exemple, les malwares intelligents ou les deepfakes peuvent tromper les mécanismes de sécurité et les utilisateurs eux-mêmes, rendant la prévention et la détection plus difficiles.

La sécurisation des environnements cloud constitue également une problématique majeure. Avec le recours massif au cloud computing, les données sont souvent stockées dans des centres répartis à travers le monde, ce qui complique la gestion des accès et la conformité aux réglementations locales et internationales telles que le RGPD ou la directive NIS2. La confiance envers les fournisseurs de services cloud et la maîtrise des configurations de sécurité sont essentielles pour éviter les vulnérabilités.

Ces défis complexes exigent une approche globale combinant technologies avancées, gouvernance rigoureuse, formation continue des utilisateurs et adaptation constante aux

évolutions réglementaires et techniques. Seule une stratégie intégrée permettra de renforcer efficacement la sécurité des données et de lutter contre les cyberattaques dans un paysage numérique en perpétuelle mutation[49].

Conclusion

À l'heure où le numérique façonne en profondeur les interactions sociales, économiques et administratives, la question de la protection des données personnelles revêt une importance stratégique croissante. L'usage massif des technologies de l'information, la numérisation des services publics et privés, ainsi que le développement de nouvelles formes de traitement automatisé des données, ont profondément transformé la relation entre les individus et les institutions.

En effet, le Maroc s'est inscrit dans cette dynamique mondiale en adoptant, dès 2009, la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette loi, accompagnée de la création de la CNDP, a marqué une avancée significative dans le paysage juridique marocain.

Notre recherche s'est inscrite dans une démarche d'analyse critique de ce dispositif, en confrontant le cadre juridique et institutionnel existant à la réalité de sa mise en œuvre sur le terrain. L'objectif principal a été d'examiner dans quelle mesure la protection des données personnelles, telle qu'elle est encadrée par le droit marocain, est effectivement assurée dans les pratiques des structures publiques et privées.

La méthodologie adoptée repose sur une approche qualitative, fondée sur une démarche pratique fondée sur l'analyse de cas réels. L'étude a ainsi mis en évidence plusieurs constats majeurs. Sur le plan normatif, la loi 09-08 présente un ensemble de dispositions qui, bien que pionnières à leur époque, apparaissent aujourd'hui partiellement dépassées face aux évolutions rapides du droit international et européen, notamment avec l'entrée en vigueur du RGPD dans l'Union européenne. L'absence de certains droits pour les personnes concernées, l'insuffisance des obligations imposées aux responsables de traitement, ou encore la faiblesse du régime de sanction, illustrent les limites du cadre juridique actuel.

Au terme de ce étude, il apparaît clairement que la protection des données personnelles au Maroc repose sur un cadre juridique dont l'ambition initiale est indéniable, mais qui peine à répondre aux exigences actuelles d'un environnement numérique complexe, transfrontalier et évolutif. La mise en œuvre du droit reste inégale, fragmentée et dépend largement de la volonté et des capacités des structures concernées. Ce constat appelle une réflexion approfondie sur les ajustements nécessaires, tant au niveau normatif qu'institutionnel et opérationnel.

En définitive, la protection des données personnelles ne peut être dissociée d'une vision stratégique plus large du numérique, articulant souveraineté, sécurité, innovation et droits fondamentaux. Cet article espère avoir apporté, à son échelle, une contribution utile à cette réflexion, en éclairant les dynamiques et les limites d'un dispositif en constante évolution.

[49] https://fr.scribd.com/document/872753483/Incident-de-Piratage-de-La-CNSS-Avril-2025, consulté le 01/06/26

REFERENCES

Ouvrages :

- BENSOUSSAN A., La protection des données personnelles de A à Z, Bruxelles, Éditions ELS Belgium s.a., 2017.

-BLANCHET A. et GOTMAN A., L'enquête et ses méthodes : l'entretien, Paris, Armand Colin, 2010.

-PAILLÉ P. et MUCCHIELLI A., L'analyse qualitative en sciences humaines et sociales, Paris, Armand Colin, 2016.

-BADIL M., « Dispositif juridique et institutionnel en matière de lutte contre la Cybercriminalité au Maroc -Défis et perspectives- », 1er édition 2022.

-DIK A., « La fraude informatique au Maroc », Librairie DAR ASSALAM, Rabat, 1ère édition.

-ENNASHI K., « la criminalité numérique droit marocain », Librairie RACHAD, Settat, 1ère édition 2020.

- ZICRY L., « Cyber -risques, le nouvel enjeu du secteur bancaire et financier », les essentiels de la banque et de la finance, RB Edition, Paris, 2017.

Revues et articles :

-AAKOUR S. & al. (2023) « PROTECTION DES DONNEES PERSONNELLES ET CYBERSECURITE », Revue Internationale du Chercheur « Volume 4 : Numéro 3 ».

-AAKOUR S., « L'ÉTENDUE DE LA PROTECTION PÉNALE DES SYSTÈMES DE TRAITEMENT AUTOMATISÉ DES DONNÉES ».

-ELLOUMI A., « La protection des données à caractère personnel sur l'Internet ».

-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 ».

-Olivier de Maison Rouge, La fraude & la recherche de la preuve, / REVUE DES DIRECTEURS SÉCURITÉ D'ENTREPRISE, N° 21, JANVIER 2016.

-ATROUCH B., La protection des données personnelles du salarié, Journal of Integrated Studies In Economics, Law, Technical Sciences & Communication, Vol(1), No (1) 2021.

-BOULAFDOUR B., La gouvernance des systèmes d'information au Maroc : une étude empirique, Revue du Contrôle de la Comptabilité et de l'Audit, Numéro 6 : Septembre 2018.

-KOUNAIDI H., MAZOUZ Y., KOUNAIDI M., « Impact de la loi 09-08 sur la gouvernance des systèmes d'information des administrations publiques marocaines », Revue du Contrôle de la Comptabilité et de l'Audit, Numéro 7 : Décembre 2018.

-Revue du droit et des affaires internationales, avril 2020, N°27, DLA piper Casablanca

-Revue Marocaine d'administration locale et de développement, REMALD, 101 Novembre-Décembre 2011.

- La nouvelle loi sur la protection des données physiques », Newsletter de Garrigues, Maroc N° 7 avril Mai et juin 2009.

-Le meilleur des revues Dalloz « Grand Angle », Le RGPD. Edition 2018, coordination éditoriale :Prévost S. et Royer E.

Textes de lois :

-Décret n° 2-21-406, le comité stratégique de la cybersécurité. Dahir n° 1-20-100 du 16 joumada 1 1442 (31 décembre 2020) portant promulgation de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques.
-Dahir n°1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05- 20 relative à la cybersécurité, B.O n° 6906, 16 hija 1441 (6-8-2020), p 1294.
-Décret n° 2-11-509 du 21 septembre 2011, rattaché à la création de La Direction Générale de la Sécurité des Systèmes d'Information.
-Dahir n° 1-11-03 du 14 rabii I 1432 (18 février 2011) portant promulgation de laloi n° 31-08 édictant des mesures de protection du consommateur.
-Dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi n° 53-05 relative à l'échange électronique de données juridiques.
-Convention 108 + pour la protection des personnes à l'égard du traitement des données à caractère personnel.
-Convention n° 108 du Conseil de l'Europe pour la protection des personnes physiques a l'égard du traitement des données à caractère personnel.
-Règlement Général relatif à la protection des données personnelles : règlement européen n 2016/679 du Parlement européen du Conseil 27 avril 2016.

Rapports :

-LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CADRE DU SECTEUR DE LA SÉCURITÉ AU MAROC ; Séminaire DCAF - CEDHD 19 et 20 octobre 2015 Ŕ Rabat, Maroc.
-Rapport d'activité de la CNDP 2014, Senso Unico éditions, Rabat, les presses de Kawtar Print Mohammedia, 2015.
-Rapport d'activité de la CNDP, 2010-2013.
-Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.