

Réflexion sur La Digitalisation de l'administration publique et la protection des données personnelles Au Maroc : loi 09.08 comme pré requis

The Digitalization of Public Administration and the Protection of Personal Data in Morocco:
An Analysis of Law No. 09.08 as a Fundamental Prerequisite for Successful Digital Transformation.

AMAR AHMED

Doctorant à l'université Mohammed 5 Rabat – Souissi

Equipe de recherche : ERPAPF

Option : Droit public

ahmedamar@um5.ac.ma

Résumé

La digitalisation est un processus de modernisation qui transforme profondément le fonctionnement des administrations et des organisations en intégrant les technologies numériques. Elle permet de simplifier les démarches, d'améliorer l'efficacité des services publics, de réduire les coûts et de faciliter l'accès à l'information pour les citoyens.

Au Maroc, cette transformation s'inscrit dans une dynamique de modernisation de l'administration publique, mais elle reste confrontée à plusieurs défis. Sur le plan technique et administratif, on note des limites liées aux infrastructures, au manque d'interopérabilité des systèmes et aux compétences numériques insuffisantes. Sur le plan juridique et éthique, la protection des données personnelles, encadrée par la loi 09-08 et supervisée par la CNDP Maroc, reste un enjeu majeur, notamment face aux risques de cyberattaques et à l'évolution rapide des technologies.

La cybersécurité représente également un défi important, car les systèmes numériques sont exposés à des menaces telles que le piratage, le phishing et les fuites de données. Cela nécessite des mesures de protection renforcées, ainsi qu'une sensibilisation continue des utilisateurs et des responsables.

la réussite de la transformation numérique dépend de la modernisation du cadre juridique, du renforcement des infrastructures, de la formation des acteurs et de l'adoption d'une culture numérique responsable. Dans ce contexte, la digitalisation apparaît comme un levier essentiel de développement, mais elle doit être encadrée pour garantir la sécurité, la transparence et le respect des droits des citoyens dans le cadre de la Transformation numérique.

Mots-clés :

Digitalisation ; Administration publique ; Transformation numérique ; Protection des données personnelles ; Loi 09-08 ; Cybersécurité ; Gouvernance numérique.

Abstract :

Digitalization is a modernization process that profoundly transforms the functioning of administrations and organizations through the integration of digital technologies. It helps

simplify administrative procedures, improve the efficiency of public services, reduce operational costs, and facilitate citizens' access to information.

In Morocco, this transformation is part of a broader effort to modernize public administration with the aim of providing more efficient, transparent, and accessible services. However, it still faces several challenges. From a technical and administrative perspective, limitations remain due to insufficient digital infrastructure, the lack of interoperability between information systems, and sometimes inadequate digital skills among stakeholders.

From a legal and ethical standpoint, the protection of personal data remains a major concern. Governed by Law No. 09-08 and supervised by the National Commission for the Control of Personal Data Protection (CNDP), data protection aims to ensure the confidentiality and security of citizens' information in the face of increasing digital data processing activities.

Furthermore, cybersecurity represents a significant challenge, as digital systems are exposed to various threats such as hacking, phishing, malware, and data breaches. This situation requires the implementation of stronger security measures as well as continuous awareness and training programs for public officials, administrative staff, and citizens regarding cybersecurity best practices.

In conclusion, the success of digital transformation depends on several key factors, including the modernization of the legal framework, the strengthening of technological infrastructure, the training of stakeholders, and the promotion of a responsible digital culture. In this context, digitalization appears to be a strategic lever for development and modernization, provided that it guarantees system security, service transparency, and the protection of citizens' fundamental rights.

Keywords:

Digitalization; Public Administration; Digital Transformation; Personal Data Protection; Law No. 09-08; Cybersecurity; Digital Governance.

Introduction :

La révolution numérique a profondément transformé les modes de fonctionnement des sociétés modernes, notamment dans le domaine de l'administration publique. Face aux exigences croissantes des citoyens en matière de rapidité, de transparence et d'efficacité, plusieurs États ont adopté des stratégies de digitalisation afin de moderniser leurs services administratifs. Le Maroc, à son tour, s'est engagé dans cette dynamique de transformation numérique à travers la mise en place de plateformes électroniques, de procédures dématérialisées et de services publics accessibles en ligne. Cette évolution vise non seulement à simplifier les démarches administratives, mais également à renforcer la bonne gouvernance, réduire la bureaucratie et améliorer la relation entre l'administration et les usagers.

Dans ce contexte, la digitalisation de l'administration publique apparaît comme un outil essentiel de développement économique et social. Elle permet une meilleure circulation de l'information, une réduction des coûts et des délais administratifs, ainsi qu'une plus grande accessibilité des services publics, même à distance. Les citoyens peuvent désormais effectuer plusieurs démarches administratives sans se déplacer, telles que le paiement des taxes, l'obtention de documents administratifs ou encore l'accès à certains services sociaux et fiscaux. Cette modernisation contribue également à renforcer la transparence administrative et à limiter certaines pratiques liées à la corruption ou aux lourdeurs bureaucratiques¹.

Cependant, cette transformation numérique entraîne également de nouveaux défis, particulièrement en matière de protection des données personnelles. En effet, les administrations publiques collectent et traitent quotidiennement une quantité considérable d'informations sensibles concernant les citoyens : données d'identité, informations fiscales, dossiers médicaux, données biométriques ou encore informations sociales et professionnelles. L'utilisation croissante des systèmes numériques expose ainsi ces données à divers risques tels que le piratage informatique, les cyberattaques, les fuites d'informations ou l'utilisation abusive des données personnelles.

Malgré les efforts entrepris, plusieurs défis demeurent encore présents, notamment le renforcement de la cybersécurité, la sensibilisation des citoyens à leurs droits numériques, la modernisation des infrastructures technologiques ainsi que l'adaptation continue du cadre juridique face à l'évolution rapide des technologies. Dès lors, la question de la protection des données personnelles devient indissociable du processus de digitalisation de l'administration publique. Il apparaît donc essentiel de trouver un équilibre entre innovation numérique, efficacité administrative et respect des libertés individuelles afin d'assurer une transition numérique sécurisée et durable au Maroc².

L'intérêt de notre sujet s'inscrit clairement dans le débat de la marge de l'administration publique, autrement dit sa capacité d'accueil et de sauvegarde en matière de

¹ Gilles Babinet , 2020 , Refondre les politiques publiques avec le numérique, *La transformation digitale de l'administration publique marocaine : perception des usagers* (2022).

² Gilles Babinet , 2020 , Refondre les politiques publiques avec le numérique , *La transformation digitale de l'administration publique marocaine : perception des usagers* (2022).

numérisation compte tenu de l'augmentation continue des mutations institutionnelles, Au-delà dans quelle mesure la mutualisation des efforts des Responsables et conscience des administrés peuvent-ils contribuer à la concrétisation et la généralisation des dispositions de la loi 08.09 au niveau des administrations et services gouvernementales ?

Partie 1 : digitalisation de l'administration publique au Maroc

La digitalisation de l'administration publique au Maroc s'inscrit dans une dynamique de modernisation de l'action publique et de renforcement de la qualité des services offerts aux citoyens et aux entreprises. Face aux évolutions technologiques et aux attentes croissantes des usagers, l'État marocain a entrepris plusieurs réformes visant à intégrer les technologies numériques dans le fonctionnement des administrations publiques. Cette transformation a pour objectif de simplifier les procédures administratives, réduire les délais de traitement des dossiers, améliorer l'efficacité des services publics et promouvoir davantage de transparence dans les relations entre l'administration et les citoyens.

Au cours des dernières années, le Maroc a développé plusieurs plateformes numériques permettant d'effectuer à distance diverses démarches administratives, telles que les déclarations fiscales, les demandes de documents administratifs, les paiements électroniques ou encore certains services liés à l'état civil. Ces initiatives ont contribué à réduire les déplacements des usagers, à limiter les lourdeurs bureaucratiques et à améliorer l'accessibilité des services publics.

outefois, malgré les progrès réalisés, la digitalisation de l'administration publique demeure confrontée à plusieurs défis. Parmi ceux-ci figurent la fracture numérique entre les différentes régions du Royaume, l'insuffisance des compétences numériques chez certains citoyens et agents publics, ainsi que les enjeux liés à la cybersécurité et à la protection des données personnelles. De plus, l'interconnexion entre les différentes administrations reste un chantier important afin de garantir une meilleure circulation de l'information et une plus grande efficacité administrative.

Malgré ces contraintes, la transformation numérique représente une opportunité majeure pour renforcer la performance de l'administration marocaine et améliorer la gouvernance publique. Elle permet non seulement d'offrir des services plus rapides et plus accessibles, mais également de renforcer la confiance des citoyens envers les institutions publiques. Dans cette perspective, la poursuite des investissements dans les infrastructures numériques, la formation des ressources humaines et l'accompagnement des usagers constituent des conditions essentielles pour assurer le succès de cette transition et construire une administration moderne, efficace et orientée vers les besoins des citoyens.¹

1- Définition et objectifs de la digitalisation :

La digitalisation désigne le processus par lequel les technologies numériques sont intégrées dans les activités, les services et les modes de fonctionnement des organisations afin

¹ Gilles J. Guglielmi, Luca Belli , *L'État digital : numérisation de l'administration publique et administration du numérique* , 2022.

d'améliorer leur efficacité, leur performance et leur capacité à répondre aux besoins des usagers. Dans le secteur public, elle se traduit par la transformation des procédures administratives traditionnelles en services numériques accessibles à distance grâce à Internet et aux outils informatiques. Cette évolution permet de remplacer progressivement les démarches papier par des procédures dématérialisées, plus rapides et plus simples à utiliser.

La digitalisation est devenue un enjeu majeur pour les administrations publiques dans un contexte marqué par l'évolution rapide des technologies de l'information et de la communication. Les citoyens sont aujourd'hui de plus en plus exigeants en matière de qualité, de rapidité et d'accessibilité des services publics. Face à ces attentes, les administrations doivent moderniser leurs méthodes de travail afin de garantir un service plus efficace et mieux adapté aux besoins de la population.

Les objectifs de la digitalisation sont nombreux. Elle vise tout d'abord à améliorer la qualité des services publics en facilitant l'accès aux prestations administratives et en réduisant les délais de traitement des demandes. Grâce aux plateformes numériques, les citoyens peuvent accomplir certaines démarches à distance, sans avoir à se déplacer ou à attendre longtemps dans les administrations. Cette simplification des procédures permet de gagner du temps aussi bien pour les usagers que pour les agents publics.

La digitalisation a également pour objectif de renforcer la transparence et la bonne gouvernance. En numérisant les procédures administratives, il devient plus facile de suivre le traitement des dossiers et de garantir une meilleure traçabilité des opérations. Cela contribue à réduire les risques d'erreurs, d'abus ou de corruption, tout en renforçant la confiance des citoyens envers l'administration.

Par ailleurs, la transformation numérique permet une meilleure gestion des ressources publiques. La réduction de l'utilisation du papier, l'automatisation de certaines tâches et l'amélioration de la circulation de l'information contribuent à diminuer les coûts de fonctionnement et à accroître la productivité des administrations. Elle favorise également une meilleure coordination entre les différents services publics grâce au partage rapide et sécurisé des données¹.

Enfin, la digitalisation constitue un facteur essentiel de modernisation et de développement. Elle permet aux administrations de s'adapter aux évolutions technologiques, de répondre plus efficacement aux besoins des citoyens et de soutenir la compétitivité économique du pays. Toutefois, pour atteindre pleinement ces objectifs, il est nécessaire de garantir l'accès aux outils numériques pour tous, de renforcer les compétences digitales des usagers et des fonctionnaires, et d'assurer un niveau élevé de sécurité des systèmes d'information.

En somme, la digitalisation représente aujourd'hui un levier stratégique de transformation de l'administration publique. Elle contribue à la construction d'une administration plus moderne, plus performante, plus transparente et davantage orientée vers la satisfaction des citoyens².

¹ Christelle Perrin , La fonction publique face à la digitalisation , 2023 .

² *La transformation digitale de l'administration publique marocaine en temps de crise* (2024).

2- stratégies numériques adoptées par le Maroc

Conscient de l'importance du numérique dans le développement économique et administratif, le Maroc a mis en place plusieurs stratégies visant à accélérer sa transformation digitale et à moderniser les services publics. Ces stratégies ont pour objectif de faire du numérique un levier de croissance, d'amélioration de la gouvernance et de renforcement de la compétitivité du pays.

L'une des premières initiatives majeures a été la stratégie Maroc Numeric 2013, lancée en 2009. Cette stratégie visait à développer l'usage des technologies de l'information et de la communication, à faciliter l'accès des citoyens aux services numériques et à renforcer l'administration électronique. Elle s'articulait autour de plusieurs axes, notamment la transformation de l'administration publique, le développement de l'économie numérique et la réduction de la fracture numérique.

Par la suite, le Maroc a poursuivi ses efforts à travers le Plan Maroc Digital et différentes réformes destinées à accompagner l'évolution technologique du pays. Ces initiatives ont permis la mise en place de nombreuses plateformes numériques destinées aux citoyens, aux entreprises et aux administrations, favorisant ainsi la dématérialisation progressive des procédures administratives.

Parallèlement, plusieurs programmes ont été lancés pour soutenir cette transformation, notamment la création de plateformes de services publics en ligne, le développement de l'identité numérique, la généralisation du paiement électronique et la promotion de l'open data. L'objectif est de rendre l'administration plus efficace, plus transparente et plus proche des citoyens tout en favorisant un environnement propice à l'innovation et à l'investissement.

3-les avantages de la digitalisation

La digitalisation constitue aujourd'hui un axe stratégique majeur de modernisation de l'administration publique au Maroc. Elle vise à transformer les modes de gestion traditionnels en des services plus rapides, accessibles et efficaces, afin de répondre aux attentes croissantes des citoyens et des entreprises.

Dans l'administration marocaine, la digitalisation permet d'abord de simplifier les démarches administratives. De nombreux services sont désormais accessibles en ligne (état civil, fiscalité, démarches sociales, inscriptions, certificats), ce qui réduit les déplacements physiques et les files d'attente dans les administrations. Cela améliore considérablement l'expérience des usagers et rapproche l'administration du citoyen.

Elle contribue également à une meilleure efficacité interne des institutions publiques. Grâce à la dématérialisation des documents et à la centralisation des données, les échanges entre administrations deviennent plus fluides et plus rapides. Cela limite les doublons, réduit les erreurs de traitement et améliore la coordination entre les différents services publics.

Sur le plan économique, la digitalisation permet à l'administration marocaine de réduire les coûts liés au papier, à l'archivage physique et aux procédures lourdes. Elle favorise aussi une gestion plus transparente des ressources publiques, en renforçant la traçabilité des opérations administratives.

Par ailleurs, cette transformation numérique renforce la transparence et la bonne gouvernance. Les procédures digitalisées laissent des traces numériques, ce qui réduit les risques d'irrégularités et améliore la confiance des citoyens envers les institutions publiques.

Enfin, la digitalisation s'inscrit dans une dynamique nationale de modernisation globale, portée par la transformation numérique du pays, visant à améliorer la compétitivité, encourager l'innovation et développer des services publics plus performants et inclusifs.

Partie II – La protection des données personnelles au Maroc

La protection des données personnelles au Maroc est devenue un enjeu fondamental avec l'accélération de la digitalisation des services publics et privés. Elle consiste à garantir la confidentialité, la sécurité et la bonne utilisation des informations personnelles des citoyens, afin d'éviter tout usage abusif, fraude ou atteinte à la vie privée.

Au Maroc, ce domaine est encadré principalement par la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette loi définit les règles que doivent respecter toutes les structures (administrations, entreprises, associations, plateformes numériques) lorsqu'elles collectent et traitent des données personnelles. Elle repose sur plusieurs principes essentiels : la légitimité du traitement, la finalité précise des données, la proportionnalité (ne collecter que les données nécessaires), la durée limitée de conservation et surtout le consentement de la personne concernée dans de nombreux cas.

Pour assurer l'application de cette loi, le Maroc dispose de la CNDP Maroc, qui joue un rôle central. Elle est chargée de contrôler les traitements de données, de délivrer des autorisations ou des déclarations, de conseiller les institutions publiques et privées, et de sensibiliser les citoyens à leurs droits numériques. Elle peut également intervenir en cas de non-respect de la loi et appliquer des sanctions.¹

Avec le développement rapide des services numériques tels que l'e-administration, les applications mobiles, les services bancaires en ligne, l'e-commerce et les plateformes de santé ou d'éducation, la question de la protection des données est devenue encore plus sensible. En effet, la multiplication des échanges de données augmente les risques de piratage, de fuite d'informations ou d'usurpation d'identité.

Dans ce contexte, la protection des données personnelles contribue directement à renforcer la confiance des citoyens dans la digitalisation. Sans sécurité des données, l'utilisation des services numériques serait limitée et risquée. Elle est donc un pilier essentiel de la transformation numérique et de la modernisation de l'État.

Le Maroc poursuit également ses efforts pour adapter son cadre juridique aux standards internationaux, notamment en s'inspirant des bonnes pratiques européennes en matière de protection des données. Cela permet de mieux encadrer les nouvelles technologies

¹ *Étude sur l'interopérabilité comme catalyseur de la digitalisation de l'administration publique au Maroc* (2025).

comme le cloud computing, l'intelligence artificielle et le traitement massif des données (big data).

Ainsi, la protection des données personnelles s'inscrit pleinement dans la dynamique de la Transformation numérique, en cherchant à concilier innovation technologique, modernisation des services et respect des droits fondamentaux des citoyens.

1- Notion des données personnelles

Les données personnelles désignent l'ensemble des informations qui permettent d'identifier, directement ou indirectement, une personne physique. Autrement dit, toute donnée qui se rapporte à un individu et qui peut permettre de le reconnaître entre dans cette catégorie. Cela peut être des informations simples comme le nom, le prénom, l'adresse, le numéro de téléphone, la date de naissance ou le numéro de carte d'identité, mais aussi des éléments plus techniques ou numériques comme l'adresse IP, la localisation géographique, les identifiants en ligne ou encore les cookies utilisés lors de la navigation sur internet.

La notion de données personnelles est donc très large, car elle ne se limite pas uniquement aux informations explicites. Même des données prises séparément peuvent sembler anonymes, mais lorsqu'elles sont croisées entre elles, elles peuvent permettre d'identifier une personne. Par exemple, la combinaison d'un âge, d'une ville et d'une profession peut suffire à reconnaître un individu dans certains cas.

On distingue généralement plusieurs types de données personnelles. D'abord, les données d'identification qui concernent l'identité de la personne. Ensuite, les données de contact qui permettent de joindre l'individu. Il existe aussi les données sensibles, qui sont particulièrement protégées car elles touchent à la vie privée profonde, comme les informations médicales, les opinions politiques, la religion ou l'origine sociale. Enfin, les données numériques concernent l'activité en ligne des utilisateurs, comme les recherches effectuées, les sites visités ou les interactions sur les réseaux sociaux.

Avec le développement rapide de la digitalisation et de la Transformation numérique, la collecte et l'utilisation des données personnelles sont devenues omniprésentes dans la société moderne. Elles sont utilisées dans de nombreux domaines comme les administrations publiques, les banques, les entreprises, les hôpitaux ou encore les plateformes numériques. Cela permet d'améliorer les services, de personnaliser les offres et de faciliter les démarches, mais cela augmente aussi les risques liés à la vie privée.

C'est pourquoi la protection des données personnelles est devenue une priorité. Au Maroc, ce domaine est encadré par la loi 09-08 et supervisé par la CNDP Maroc. Cette institution veille à ce que les données soient collectées de manière légale, utilisées uniquement pour des finalités précises et protégées contre tout accès non autorisé.

Ainsi, les données personnelles représentent un élément fondamental de la société numérique actuelle. Elles sont au cœur des échanges d'information et du fonctionnement des services modernes, mais nécessitent un encadrement strict afin de garantir le respect de la vie privée et la sécurité des individus dans un monde de plus en plus digitalisé.

2- Cadragé juridique au Maroc (loi 09.08)¹

Le cadragé juridique de la protection des données personnelles au Maroc repose principalement sur la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette loi constitue le cadre légal de référence qui encadre la collecte, le traitement, le stockage et l'utilisation des données personnelles par les organismes publics et privés.

Cette loi a pour objectif principal de protéger la vie privée des citoyens et de garantir que leurs données ne soient pas utilisées de manière abusive ou illégale. Elle impose plusieurs principes fondamentaux. Tout d'abord, le principe de finalité, selon lequel les données doivent être collectées pour un objectif précis et légitime, et ne peuvent pas être utilisées pour d'autres usages sans consentement. Ensuite, le principe de proportionnalité, qui oblige les organismes à ne collecter que les données strictement nécessaires. La loi impose également la durée limitée de conservation des données, afin d'éviter leur stockage excessif, ainsi que le respect de la sécurité et de la confidentialité des informations.

Un autre principe important est celui du consentement. Dans de nombreux cas, le traitement des données personnelles nécessite l'accord préalable de la personne concernée, ce qui renforce le contrôle des individus sur leurs informations personnelles. La loi garantit également des droits aux citoyens, notamment le droit d'accès à leurs données, le droit de rectification en cas d'erreur et, dans certains cas, le droit d'opposition au traitement.

Pour assurer l'application de ce cadre juridique, le Maroc a mis en place la CNDP Maroc. Cette autorité indépendante joue un rôle central dans le contrôle et la régulation des traitements de données. Elle délivre des autorisations ou reçoit des déclarations de traitement, sensibilise les acteurs publics et privés, et veille au respect de la loi. Elle peut également prononcer des sanctions en cas de non-conformité.

Le champ d'application de la loi 09-08 est large, car il concerne aussi bien les administrations publiques que les entreprises privées, les associations et même certains organismes internationaux opérant sur le territoire marocain. Cela permet d'assurer une protection globale et uniforme des données personnelles.

Dans le contexte actuel de la transformation numérique et de la Transformation numérique, ce cadre juridique joue un rôle essentiel. Avec la montée en puissance des services numériques, de l'e-administration, du commerce électronique et des plateformes digitales, la loi 09-08 permet d'encadrer ces usages et de renforcer la confiance des citoyens dans les systèmes numériques.

Ainsi, le cadragé juridique marocain en matière de données personnelles vise à concilier deux objectifs essentiels : **encourager le développement du numérique tout en garantissant la protection des droits fondamentaux des individus, notamment leur vie privée et la sécurité de leurs informations personnelles.**

3- Le rôle de la commission Nationale de données personnelles (CNDP)

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

La **CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel)** est l'autorité chargée de garantir le respect de la loi 09-08 au Maroc en matière de protection des données personnelles. Son rôle principal est d'assurer que toutes les données collectées et traitées par les administrations publiques, les entreprises privées ou toute autre organisation soient utilisées de manière légale, sécurisée et respectueuse de la vie privée des citoyens.

De manière générale, la CNDP exerce un rôle de régulation et de contrôle. Elle veille à ce que les traitements de données respectent les principes fondamentaux de la loi, notamment la transparence, la finalité des données, la proportionnalité et la sécurité. Avant la mise en place de certains traitements, elle peut exiger une déclaration ou délivrer une autorisation, afin de s'assurer de leur conformité.

Elle joue également un rôle important dans la protection des droits des citoyens. Chaque individu dispose de droits sur ses données personnelles, comme le droit d'accès, de rectification et d'opposition. La CNDP veille à ce que ces droits soient respectés et peut intervenir en cas de violation ou de plainte.

En plus de son rôle de contrôle, la CNDP a une mission de sensibilisation et d'accompagnement.¹ Elle informe les institutions et les entreprises sur les bonnes pratiques à adopter pour protéger les données personnelles et accompagne la transition vers des systèmes numériques conformes à la loi.

Enfin, elle dispose d'un pouvoir de sanction en cas de non-respect des règles, ce qui lui permet de renforcer l'application effective de la loi et de garantir un environnement numérique plus sûr et plus fiable.

Ainsi, la CNDP constitue un acteur central de la gouvernance numérique au Maroc, car elle assure l'équilibre entre le développement de la digitalisation et la protection de la vie privée des citoyens dans le cadre de la Transformation numérique.

Partie III – Défis majeurs de la digitalisation et de la protection des données personnelles :

La digitalisation et la protection des données personnelles représentent aujourd'hui des enjeux majeurs, mais elles font face à plusieurs défis importants, notamment dans le contexte de la transformation numérique des administrations et des entreprises.

Tout d'abord, l'un des principaux défis est celui de la **cybersécurité**. Avec l'augmentation des services numériques et des échanges de données, les risques de piratage, de vol de données, de fraude ou d'usurpation d'identité deviennent de plus en plus fréquents. Les systèmes doivent donc être constamment mis à jour et sécurisés pour éviter toute faille.

Ensuite, on trouve le défi de la **sensibilisation et de la culture numérique**. Beaucoup d'utilisateurs et même certaines organisations ne maîtrisent pas encore suffisamment les bonnes pratiques en matière de protection des données. Cela peut entraîner des erreurs

¹ La transformation digitale de l'administration publique marocaine : perception des usagers (2022).

humaines, comme le partage involontaire d'informations sensibles ou l'utilisation de mots de passe faibles.

Un autre défi important est celui de la **mise en conformité juridique**. Les administrations et les entreprises doivent respecter des règles strictes, notamment celles liées à la loi 09-08¹ et aux recommandations de la CNDP Maroc. Cependant, l'adaptation des systèmes informatiques à ces exigences peut être complexe et coûteuse.

Il existe également le défi de la **gestion des volumes massifs de données (big data)**. Aujourd'hui, les données sont produites en très grande quantité, ce qui rend leur stockage, leur traitement et leur protection plus difficiles, surtout lorsqu'il s'agit de garantir leur confidentialité.

Par ailleurs, la digitalisation soulève le défi de la **confiance des utilisateurs**. Les citoyens doivent être rassurés sur le fait que leurs données personnelles sont utilisées de manière transparente et sécurisée. Sans cette confiance, l'adoption des services numériques peut être freinée.

Enfin, un défi majeur concerne l'**évolution rapide des technologies**. Les innovations comme l'intelligence artificielle, le cloud computing ou l'Internet des objets évoluent très vite, ce qui complique l'adaptation des lois, des systèmes de sécurité et des mécanismes de contrôle.

Ainsi, la digitalisation et la protection des données personnelles, dans le cadre de la Transformation numérique, nécessitent un équilibre entre innovation, sécurité et respect des droits fondamentaux afin de relever ces défis de manière efficace.

1 – les risques liés à la cybersécurité :

Les risques liés à la cybersécurité représentent aujourd'hui un enjeu majeur dans un monde de plus en plus digitalisé, où les données circulent en permanence à travers les réseaux informatiques. Avec la généralisation des services en ligne, des applications mobiles et de l'e-administration, les systèmes deviennent plus exposés aux cyberattaques, ce qui augmente les menaces sur les utilisateurs, les entreprises et les institutions publiques.

Tout d'abord, l'un des risques les plus connus est le piratage informatique (hacking). Il consiste à accéder de manière illégale à un système informatique dans le but de voler, modifier ou détruire des données. Les hackers peuvent cibler des comptes personnels, des bases de données d'entreprises ou même des systèmes gouvernementaux, ce qui peut entraîner des conséquences graves comme la perte d'informations sensibles ou l'interruption de services essentiels.

Un autre risque très fréquent est le vol de données personnelles. Les cybercriminels cherchent à récupérer des informations confidentielles telles que les identifiants, mots de passe, numéros de carte bancaire ou données d'identité. Une fois ces données obtenues, elles peuvent être utilisées pour des fraudes financières, des usurpations d'identité ou revendues sur des plateformes ou Le phishing (ou hameçonnage) est également une menace importante. Il s'agit d'une technique de manipulation qui consiste à envoyer de faux messages (emails, SMS

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

ou liens) imitant des organismes officiels comme les banques ou les administrations. Le but est de tromper l'utilisateur afin qu'il communique volontairement ses informations personnelles ou financières.

Par ailleurs, les systèmes informatiques peuvent être infectés par des virus et logiciels malveillants (malwares). Ces programmes peuvent s'introduire dans les appareils sans que l'utilisateur s'en rende compte, provoquer des dysfonctionnements, supprimer des fichiers ou espionner les activités en ligne. Ils peuvent également ouvrir des portes aux pirates pour prendre le contrôle des systèmes.

Un autre risque de plus en plus répandu est celui des attaques par ransomware. Dans ce type d'attaque, les cybercriminels bloquent l'accès aux données ou aux systèmes d'une organisation et exigent le paiement d'une rançon pour les débloquent. Cela peut paralyser totalement une entreprise ou une administration pendant plusieurs jours, voire semaines.¹

Il existe aussi des risques liés aux failles de sécurité des systèmes. Ces failles peuvent être dues à des erreurs techniques, à des logiciels non mis à jour ou à une mauvaise configuration des réseaux. Elles offrent des portes d'entrée aux attaquants pour infiltrer les systèmes sans être détectés.

En plus des impacts techniques, les conséquences de ces risques sont souvent importantes. Ils peuvent entraîner des pertes financières importantes, une atteinte à la réputation des organisations, une perte de confiance des utilisateurs et une violation de la vie privée. Pour les administrations et les entreprises, cela peut aussi perturber la continuité des services et affecter leur efficacité.

Dans le contexte actuel de la transformation numérique et de la Transformation numérique, la cybersécurité devient donc un pilier essentiel. Elle vise à protéger les systèmes, les réseaux et les données afin de garantir un environnement numérique fiable, sécurisé et digne de confiance, surtout dans un contexte où les échanges d'informations sont de plus en plus massifs et rapides.

2- limites techniques et administratives

Les limites techniques et administratives de la digitalisation constituent des freins importants à la réussite complète de la transformation numérique, notamment dans les administrations publiques. Malgré les progrès réalisés, plusieurs obstacles continuent d'affecter la mise en place efficace des services numériques.

Sur le plan technique, la première limite est liée aux infrastructures numériques insuffisantes ou inégalement développées. Certaines administrations ou régions ne disposent pas encore d'un accès stable et rapide à internet ou de systèmes informatiques modernes. Cela crée des disparités dans la qualité des services numériques et empêche une digitalisation homogène. À cela s'ajoute le problème de l'obsolescence des équipements, car de nombreux

¹ Gilles J. Guglielmi, Luca Belli, *L'État digital : numérisation de l'administration publique et administration du numérique*, 2022.

systèmes informatiques deviennent rapidement dépassés et nécessitent des mises à jour coûteuses et régulières¹.

Une autre limite technique importante est la sécurité des systèmes d'information. Avec la multiplication des données numériques, les risques de cyberattaques, de piratage et de fuite d'informations augmentent fortement. Les administrations doivent donc investir en permanence dans des solutions de protection avancées, ce qui représente un coût élevé et une contrainte technique permanente. Par ailleurs, la complexité des systèmes numériques constitue également un défi, car les différents logiciels et bases de données ne sont pas toujours compatibles entre eux, ce qui complique l'échange et l'intégration des informations.

On peut également citer la dépendance aux fournisseurs technologiques. Certaines administrations utilisent des solutions externes (logiciels, plateformes cloud), ce qui peut limiter leur autonomie et poser des problèmes en cas de panne, de changement de prestataire ou de coût élevé de maintenance.

Sur le plan administratif, une des principales limites est la lenteur des procédures de transformation. La digitalisation nécessite une restructuration complète des méthodes de travail, ce qui implique du temps, des ressources et une forte coordination entre les différents services. Les démarches administratives traditionnelles, souvent lourdes et hiérarchisées, ralentissent parfois l'adoption des nouvelles technologies.

Un autre obstacle important est le manque de compétences numériques chez certains agents publics. La digitalisation exige une formation continue pour maîtriser les outils numériques, les systèmes d'information et les nouvelles pratiques de gestion. Cependant, le manque de formation ou l'insuffisance des programmes de renforcement des capacités limite souvent l'efficacité de la transition.

La résistance au changement constitue également une limite administrative majeure. Certains employés peuvent être réticents à abandonner les méthodes traditionnelles par peur de la complexité des outils numériques ou par manque d'accompagnement. Cette résistance ralentit l'adoption globale de la digitalisation.

En outre, il existe un problème de coordination entre les administrations. Chaque service peut utiliser ses propres systèmes, ce qui crée un manque d'interopérabilité. Cette absence d'harmonisation rend difficile le partage des données, la communication entre les institutions et la création d'une administration intégrée et efficace.

Enfin, les contraintes liées au cadre réglementaire et à la gestion administrative peuvent aussi ralentir la digitalisation. La mise en conformité avec les lois, les procédures d'autorisation et les exigences de contrôle rendent parfois les projets numériques plus longs à mettre en œuvre.

Ainsi, même si la digitalisation s'inscrit dans une dynamique de modernisation globale de la Transformation numérique, elle reste confrontée à des limites techniques et administratives importantes. Ces obstacles montrent que la réussite de la transformation

¹ Gilles J. Guglielmi, Luca Belli , *L'État digital : numérisation de l'administration publique et administration du numérique* , 2022.

numérique dépend non seulement des technologies, mais aussi de l'investissement humain, organisationnel et institutionnel.

3-défis juridiques et éthiques

Les défis juridiques et éthiques de la digitalisation sont aujourd'hui au cœur des débats liés à la transformation numérique des sociétés. En effet, si la digitalisation apporte de nombreux avantages en termes d'efficacité et de modernisation, elle soulève également des questions complexes liées au droit, à la protection des individus et aux valeurs fondamentales¹.

Sur le plan juridique, l'un des premiers défis est l'adaptation permanente du cadre légal aux évolutions technologiques. Les technologies numériques évoluent très rapidement (intelligence artificielle, big data, cloud computing, objets connectés), tandis que les lois nécessitent du temps pour être élaborées et mises en œuvre. Cela crée un décalage entre les pratiques numériques et les réglementations existantes, ce qui peut laisser certaines zones grises juridiques.

Un autre défi majeur concerne la protection des données personnelles, encadrée au Maroc par la loi 09-08 et supervisée par la CNDP Maroc. Malgré ce cadre légal, la difficulté réside dans l'application effective des règles face à la multiplication des plateformes numériques, des applications mobiles et des échanges de données transfrontaliers. De plus, les données peuvent être stockées sur des serveurs situés à l'étranger, ce qui complique le contrôle et la souveraineté numérique.

La question de la responsabilité juridique constitue également un défi important. En cas de cyberattaque, de fuite de données ou de dysfonctionnement d'un système numérique, il est parfois difficile d'identifier clairement les responsables : est-ce l'administrateur du système, le fournisseur de service, l'utilisateur ou le cybercriminel externe ? Cette complexité rend l'application des sanctions et la réparation des dommages plus difficile.

Un autre enjeu juridique important est celui de la sécurisation des échanges numériques et des transactions électroniques. Le développement de l'e-administration, de l'e-commerce et des services en ligne nécessite des garanties solides en matière d'authentification, de signature électronique et de preuve numérique afin d'assurer la fiabilité des échanges.

Sur le plan éthique, l'un des défis majeurs est la protection de la vie privée et des libertés individuelles. La collecte massive de données peut entraîner une surveillance excessive des individus, parfois sans qu'ils en soient pleinement conscients. Cela soulève des questions sur les limites à ne pas dépasser entre innovation technologique et respect de la vie privée.

Un autre défi éthique important est celui de la transparence et de l'explicabilité des algorithmes, notamment dans les systèmes d'intelligence artificielle. De plus en plus de décisions sont prises de manière automatisée (crédit bancaire, recrutement, orientation, services publics), mais les critères utilisés ne sont pas toujours compréhensibles pour les citoyens. Cela peut engendrer des risques de discrimination ou d'injustice algorithmique.

¹ *E-gouvernance et transformation numérique au Maroc : défis et perspectives (2024).*

La question de l'équité numérique est également centrale. La digitalisation peut accentuer les inégalités entre les personnes ayant accès aux technologies et celles qui en sont exclues, que ce soit pour des raisons économiques, géographiques ou de compétences numériques. Cela pose un défi éthique important pour garantir une inclusion numérique équitable.

Il existe aussi le défi de la responsabilité morale des acteurs du numérique, qu'il s'agisse des administrations ou des entreprises privées. Ces acteurs doivent veiller à utiliser les technologies de manière responsable, en évitant les abus, la manipulation des données ou l'exploitation des utilisateurs.¹

Enfin, la digitalisation pose la question de la confiance numérique. Sans confiance des citoyens dans la sécurité et l'éthique des systèmes numériques, l'adoption des services digitaux peut être limitée, ce qui freine la transformation globale de la société.

Ainsi, les défis juridiques et éthiques de la digitalisation, dans le cadre de la Transformation numérique, montrent qu'il est nécessaire de trouver un équilibre entre innovation technologique, protection des droits fondamentaux et respect des valeurs humaines, afin de construire un environnement numérique sûr, juste et durable.

Partie III- Perspectives et solutions

Les perspectives et solutions liées à la digitalisation et à la protection des données personnelles s'inscrivent dans une dynamique de modernisation continue visant à améliorer l'efficacité des services tout en garantissant la sécurité et les droits des citoyens. Elles concernent aussi bien les aspects technologiques, juridiques qu'organisationnels.

Tout d'abord l'une des principales perspectives est le renforcement de la transformation numérique des administrations publiques². Cela passe par la généralisation des services en ligne, la dématérialisation complète des procédures administratives et la création de plateformes intégrées permettant aux citoyens d'accéder facilement à leurs démarches. Cette évolution vise à rendre l'administration plus rapide, plus transparente et plus accessible.

Sur le plan technologique, une solution essentielle est le développement des infrastructures numériques sécurisées. Cela inclut l'amélioration de la qualité des réseaux internet, la modernisation des systèmes informatiques et l'investissement dans des solutions avancées de cybersécurité (pare-feu, chiffrement des données, systèmes de détection des intrusions). Ces outils permettent de réduire les risques de piratage et de fuite de données.

Une autre perspective importante est le renforcement de la gouvernance des données. Cela signifie mieux organiser la collecte, le stockage et l'utilisation des données personnelles afin de garantir leur conformité avec les lois en vigueur, notamment la loi 09-08 encadrée par la CNDP Maroc. Cette gouvernance repose sur la transparence, la responsabilité et la traçabilité des traitements de données.

¹ E-gouvernance et transformation numérique au Maroc : défis et perspectives (2024).

² E-gouvernance et transformation numérique au Maroc : défis et perspectives (2024).

Par ailleurs, la formation et la sensibilisation des utilisateurs et des agents administratifs constituent une solution fondamentale. Le développement des compétences numériques permet de réduire les erreurs humaines, d'améliorer la sécurité des systèmes et de favoriser une meilleure adoption des outils digitaux. La sensibilisation aux bonnes pratiques (mots de passe sécurisés, vigilance face au phishing, protection des données personnelles) est également indispensable.

Sur le plan juridique, une perspective importante est l'adaptation continue du cadre réglementaire afin de suivre l'évolution rapide des technologies. Cela implique de renforcer les lois existantes, d'intégrer de nouvelles réglementations pour les technologies émergentes comme l'intelligence artificielle, et d'harmoniser les règles avec les standards internationaux pour mieux encadrer les flux de données transfrontaliers.

En matière de sécurité, une solution clé est le renforcement de la cybersécurité nationale à travers la mise en place de stratégies globales de protection des systèmes d'information, la création de centres de surveillance et de réponse aux incidents, ainsi que la coopération entre les acteurs publics et privés.

Enfin, une perspective essentielle est le développement d'une culture numérique responsable et éthique. Cela consiste à promouvoir le respect de la vie privée, la transparence dans l'utilisation des données et l'équité dans les systèmes numériques, notamment ceux basés sur l'intelligence artificielle.

Ainsi, les perspectives et solutions de la digitalisation, dans le cadre de la Transformation numérique, montrent que la réussite de la transition numérique dépend d'un équilibre entre innovation, sécurité, formation et respect des droits fondamentaux, afin de construire une société numérique plus performante et plus fiable.

1- Astuces pour Renforcement de la cybersecurité

Le renforcement de la cybersécurité repose sur un ensemble de bonnes pratiques techniques et comportementales visant à protéger les systèmes informatiques, les réseaux et les données contre les cyberattaques. Dans un contexte de digitalisation croissante, ces mesures deviennent indispensables pour garantir la sécurité des informations et la continuité des services¹.

Tout d'abord, l'un des éléments fondamentaux est l'utilisation de **mots de passe forts et uniques**. Un mot de passe sécurisé doit être suffisamment long et complexe, combinant lettres, chiffres et caractères spéciaux. Il est également recommandé d'utiliser un mot de passe différent pour chaque compte afin d'éviter qu'une seule faille de sécurité compromette plusieurs services en même temps. L'utilisation de gestionnaires de mots de passe peut aussi faciliter cette pratique.

Ensuite, l'authentification à deux facteurs constitue une mesure très efficace pour renforcer la sécurité des comptes. Elle ajoute une étape supplémentaire de vérification, comme un code envoyé par SMS ou généré par une application. Même si un mot de passe est volé, l'accès au compte reste protégé grâce à cette deuxième validation.

¹ *Étude sur l'interopérabilité comme catalyseur de la digitalisation de l'administration publique au Maroc* (2025).

La mise à jour régulière des systèmes et logiciels est également essentielle. Les mises à jour permettent de corriger des failles de sécurité et d'améliorer la protection contre les nouvelles menaces. Négliger ces mises à jour expose les systèmes à des risques importants de piratage.

Un autre aspect crucial concerne la vigilance face aux emails et liens suspects, notamment les tentatives de phishing. Les cybercriminels utilisent souvent de faux messages imitant des institutions officielles pour tromper les utilisateurs et obtenir leurs données personnelles. Il est donc important de ne jamais cliquer sur des liens inconnus ou ouvrir des pièces jointes douteuses.

L'installation d'un antivirus performant et d'un pare-feu est aussi une mesure indispensable. L'antivirus permet de détecter et supprimer les logiciels malveillants, tandis que le pare-feu contrôle les connexions réseau afin de bloquer les accès non autorisés.

La sauvegarde régulière des données constitue une autre bonne pratique essentielle. En cas de cyberattaque, de panne ou de perte de données, les sauvegardes permettent de récupérer les informations importantes. Elles peuvent être stockées sur des disques externes ou dans des solutions cloud sécurisées.

Il est également important de limiter le partage des données personnelles, notamment sur les réseaux sociaux et les plateformes en ligne. Plus les informations sont exposées, plus le risque d'usurpation d'identité ou de fraude augmente.

L'utilisation de réseaux sécurisés est une autre recommandation importante. Les connexions Wi-Fi publiques non protégées peuvent être facilement interceptées par des pirates. Dans ce cas, l'utilisation d'un VPN permet de sécuriser la connexion et de protéger les données échangées.

Par ailleurs, la formation et la sensibilisation des utilisateurs jouent un rôle essentiel dans la cybersécurité. La majorité des cyberattaques exploitent des erreurs humaines, d'où l'importance de développer une culture numérique basée sur la vigilance et les bonnes pratiques.

Enfin, la surveillance régulière des comptes et systèmes permet de détecter rapidement toute activité suspecte, comme des connexions inhabituelles ou des transactions non autorisées, afin de réagir rapidement en cas d'incident.

Ainsi, le renforcement de la cybersécurité repose sur une combinaison de mesures techniques et de comportements responsables. Dans le contexte de la Transformation numérique, ces pratiques sont essentielles pour protéger les données, sécuriser les systèmes et garantir la confiance dans l'environnement numérique.

2- Sensibilisation des Responsables et administrés

La **sensibilisation des responsables et des administrés** constitue un élément fondamental dans la réussite de la digitalisation et dans le renforcement de la cybersécurité et de la protection des données personnelles. En effet, au-delà des outils technologiques et des cadres juridiques, le facteur humain reste l'un des maillons les plus importants de la sécurité numérique.¹

¹ La transformation digitale de l'administration publique marocaine : perception des usagers (2022).

Tout d'abord, la sensibilisation des **responsables administratifs et des décideurs** est essentielle, car ce sont eux qui définissent les orientations stratégiques et mettent en place les systèmes numériques. Ils doivent comprendre les enjeux liés à la cybersécurité, à la gestion des données et aux risques de cyberattaques. Cela leur permet de prendre des décisions éclairées concernant les investissements en infrastructures, la mise en conformité avec les lois et l'adoption de bonnes pratiques. Une bonne sensibilisation leur permet également d'intégrer la sécurité dès la conception des projets numériques, ce qui réduit les risques futurs.

Ensuite, la sensibilisation des **agents administratifs** est tout aussi importante. Ces derniers manipulent quotidiennement des données personnelles et utilisent des systèmes informatiques. Ils doivent donc être formés aux bonnes pratiques, comme la gestion sécurisée des mots de passe, la détection des emails frauduleux, la protection des documents sensibles et l'utilisation correcte des outils numériques. Une erreur humaine peut parfois suffire à provoquer une fuite de données ou une cyberattaque, d'où l'importance de leur formation continue.

Par ailleurs, la sensibilisation des **administrés (citoyens et usagers)** joue également un rôle crucial. Avec la généralisation des services en ligne, les citoyens doivent être informés des risques liés à l'utilisation du numérique, notamment le phishing, le vol d'identité ou le partage excessif d'informations personnelles. Ils doivent également connaître leurs droits en matière de protection des données et les recours possibles en cas de violation.

La sensibilisation peut se faire à travers plusieurs moyens, comme des campagnes d'information, des formations, des guides pratiques, des ateliers ou encore des plateformes numériques éducatives. Les institutions publiques, notamment la CNDP Maroc, jouent un rôle important dans cette mission en diffusant des bonnes pratiques et en renforçant la culture de la protection des données.

Dans le contexte de la transformation numérique, la sensibilisation contribue directement à réduire les risques liés aux erreurs humaines, qui sont souvent à l'origine des incidents de cybersécurité. Elle permet aussi de renforcer la confiance entre les citoyens et les institutions publiques, en assurant une utilisation plus responsable et plus sécurisée des services numériques.

Enfin, la sensibilisation favorise l'adoption réussie de la digitalisation, car elle accompagne le changement des mentalités et facilite l'acceptation des nouveaux outils technologiques. Elle constitue donc un pilier essentiel de la réussite de la Transformation numérique, en plaçant l'humain au centre de la sécurité et de la modernisation numérique.

3- Modernisation et adaptation du cadrage juridique

l'évolution rapide des technologies impose une mise à jour continue des lois et des réglementations afin de garantir un encadrement efficace, sécurisé et adapté aux nouvelles pratiques numériques.

Tout d'abord, la modernisation du cadre juridique vise à **adapter les lois existantes aux nouvelles réalités technologiques**.¹ Les textes juridiques traditionnels ont été conçus à

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

une époque où le numérique était moins développé. Aujourd'hui, avec l'essor de l'e-administration, de l'intelligence artificielle, du cloud computing et du big data, il devient nécessaire de revoir et d'actualiser les lois pour couvrir ces nouveaux usages et prévenir les risques associés.

Un aspect essentiel de cette modernisation concerne la **protection des données personnelles**. Au Maroc, la loi 09-08¹ constitue le cadre de référence, mais son application doit évoluer pour répondre aux défis actuels, notamment la circulation internationale des données et l'utilisation massive des plateformes numériques. L'objectif est de renforcer les droits des citoyens tout en assurant une utilisation responsable des données par les administrations et les entreprises, sous la supervision de la CNDP Maroc.

La modernisation juridique implique également le **renforcement de la cybersécurité sur le plan légal**. Cela passe par l'introduction de nouvelles dispositions concernant la prévention des cyberattaques, la responsabilité en cas d'incident, ainsi que les sanctions applicables aux infractions numériques. L'objectif est de créer un environnement numérique plus sûr et plus fiable.

Un autre point important est l'**harmonisation avec les normes internationales**. Dans un monde interconnecté, les échanges de données dépassent les frontières nationales. Il est donc nécessaire d'aligner le cadre juridique marocain avec les standards internationaux afin de faciliter la coopération et de mieux protéger les données dans un contexte global.

La modernisation du cadre juridique implique aussi une **simplification et une clarification des procédures administratives**. Cela permet de faciliter la mise en conformité des organismes publics et privés, tout en accélérant la mise en œuvre des projets numériques.

Par ailleurs, il est important d'intégrer dans le droit les **nouvelles technologies émergentes**, comme l'intelligence artificielle, les objets connectés ou les systèmes automatisés de décision. Ces technologies soulèvent de nouvelles questions juridiques et éthiques qui nécessitent des réponses adaptées.

Enfin, cette modernisation s'inscrit pleinement dans la dynamique de la Transformation numérique, car elle permet de concilier innovation technologique, protection des droits fondamentaux et développement d'une société numérique moderne et sécurisée.

Ainsi, l'adaptation du cadrage juridique est indispensable pour accompagner les mutations numériques, garantir la sécurité des utilisateurs et assurer un équilibre entre progrès technologique et respect des règles juridiques et éthiques.

Conclusion :

En guise de conclusion, la **digitalisation** représente aujourd'hui un levier essentiel de modernisation des administrations et des organisations, notamment au Maroc, en permettant d'améliorer la qualité des services publics, de simplifier les procédures administratives et de rapprocher l'administration des citoyens. Elle favorise également une meilleure efficacité, une réduction des coûts et une accessibilité plus large aux services grâce aux outils numériques.

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

Cependant, cette transformation s'accompagne de nombreux défis et limites. Sur le plan technique et administratif, elle est freinée par des infrastructures parfois insuffisantes, des systèmes informatiques peu interopérables, ainsi que par des résistances organisationnelles et un manque de compétences numériques. Sur le plan juridique et éthique, elle soulève des questions importantes liées à la protection des données personnelles, à la responsabilité en cas de cyberattaques, ainsi qu'au respect de la vie privée et de la transparence des traitements.

Dans ce contexte, la protection des données personnelles, encadrée par la loi 09-08 et supervisée par la CNDP Maroc, joue un rôle central pour garantir la confiance des citoyens et assurer un usage sécurisé des informations. Par ailleurs, les risques liés à la cybersécurité imposent le renforcement des dispositifs de protection, de sensibilisation et de formation pour tous les acteurs concernés, qu'ils soient responsables, agents administratifs ou usagers.

Ainsi, la réussite de la transformation numérique repose sur un équilibre entre innovation technologique, modernisation du cadre juridique, renforcement de la sécurité et développement d'une culture numérique responsable. Elle s'inscrit pleinement dans une dynamique globale de la Transformation numérique, visant à construire une administration plus performante, plus transparente et plus proche des citoyens, tout en garantissant la protection de leurs droits fondamentaux.

Bibliographie :

- **Articles :**

- *Transformation digitale de l'administration publique au Maroc : revue de littérature et état des lieux* (2020)
- *La transformation digitale de l'administration publique marocaine en temps de crise* (2024)
- *Étude sur l'interopérabilité comme catalyseur de la digitalisation de l'administration publique au Maroc* (2025)
- *E-gouvernance et transformation numérique au Maroc : défis et perspectives* (2024)
- *La transformation digitale de l'administration publique marocaine : perception des usagers* (2022)

- **Textes de lois :**

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

- **Ouvrages :**

- Hélène Bégon , *La transformation numérique des administrations* , 2021
- Christelle Perrin , *La fonction publique face à la digitalisation* , 2023
- Gilles J. Guglielmi, Luca Belli , *L'État digital : numérisation de l'administration publique et administration du numérique* , 2022
- Gilles Babinet , 2020 , *Refondre les politiques publiques avec le numérique*