African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

Gouvernance juridique des données sensibles : Réponses aux défis des technologies émergentes dans le secteur public marocain

Legal Governance of Sensitive Data : Responses to the Challenges of Emerging Technologies in the Moroccan Public Sector.

Auteur 1 : Boutaina HEMIED.
Auteur 2 : Kawtar AZIZ.
Auteur 3 : Abir OMRI.
Auteur 4 : Nawal ES-SHASSAH.
Auteur 5 : AKKOUR Soumaya.

Boutaina HEMIED (Doctorante)
Faculté des Sciences Juridiques et Politiques Settat
Université Hassan 1er de Settat

Kawtar AZIZ (Doctorante)
Faculté des Sciences Juridiques et Politiques Settat
Université Hassan 1er de Settat

Abir OMRI (Doctorante)
Faculté des Sciences Juridiques et Politiques Settat
Université Hassan 1er de Settat

Nawal ES-SHASSAH (Doctorante)
Faculté des Sciences Juridiques et Politiques Settat
Université Hassan 1er de Settat

Soumaya AKKOUR (Professeure de l'Enseignement Supérieur)
Faculté des Sciences Juridiques et Politiques de Settat
Université Hassan 1er de Settat

Déclaration de divulgation : **L'auteur n'a pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.**

Conflit d'intérêts : **L'auteur ne signale aucun conflit d'intérêts.**

Pour citer cet article : **HEMIED .B, AZIZ .K, OMRI .A, ES-SHASSAH .N & AKKOUR .S (2026) « Gouvernance juridique des données sensibles : Réponses aux défis des technologies émergentes dans le secteur public marocain », African Scientific Journal « Volume 03, Num 36 » pp: 2189 – 2213.**

DOI : 10.5281/zenodo.20829067

Résumé

La gouvernance juridique des données sensibles dans le secteur public marocain constitue un pilier essentiel de la consolidation de l'État de droit et de la modernisation de l'action publique. Elle s'inscrit dans un cadre normatif et institutionnel structuré, destiné à encadrer la collecte, le traitement et la protection des informations stratégiques, tout en assurant le respect des libertés fondamentales et des exigences de sécurité juridique. À l'épreuve des technologies émergentes, telles que l'intelligence artificielle, le Big Data et l'informatique en nuage, cette gouvernance requiert une organisation opérationnelle fondée sur des mécanismes de conformité, de contrôle et de redevabilité. L'adoption de modèles juridiques adaptés permet ainsi de concilier innovation technologique, efficacité administrative et souveraineté numérique, tout en renforçant la transparence et la confiance des citoyens dans les institutions publiques marocaines.

Mots clés : Gouvernance juridique, données sensibles, secteur public marocain, technologies émergentes, redevabilité

Abstract

The legal governance of sensitive data within Morocco's public sector constitutes a fundamental pillar in strengthening the rule of law and advancing administrative modernization. It is anchored in a structured normative and institutional framework designed to regulate the collection, processing, and protection of strategic information while safeguarding fundamental rights and ensuring legal certainty. In the context of emerging technologies, including artificial intelligence, Big Data, and cloud computing, this governance necessitates an operational organization grounded in robust compliance, oversight, and accountability mechanisms. The adoption of adaptive legal models thus enables a balanced reconciliation between technological innovation, administrative efficiency, and digital sovereignty, while enhancing transparency and fostering public trust in Moroccan institutions.

Keywords : Legal Governance, sensitive Data, Moroccan Public Sector, emerging Technologies, accountability

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

Introduction

La transformation numérique du secteur public marocain a profondément renouvelé les modalités d'exercice de l'action administrative. La dématérialisation des procédures, le développement des plateformes numériques, l'interconnexion des systèmes d'information, le recours croissant aux services cloud, ainsi que l'émergence de l'intelligence artificielle, du Big Data, de l'Internet des objets, de la biométrie et de l'analytique avancée ont placé la donnée au cœur de l'administration contemporaine. Les données traitées par les administrations publiques ne constituent plus de simples informations nécessaires à la gestion quotidienne des services publics ; elles deviennent désormais des instruments d'aide à la décision, de coordination institutionnelle, d'anticipation des besoins sociaux et d'amélioration de la performance administrative.

Toutefois, cette centralité nouvelle de la donnée s'accompagne d'une exposition accrue aux risques juridiques, techniques et institutionnels. Ces risques deviennent particulièrement sensibles lorsque les traitements portent sur des données relatives à l'identité, à la santé, à la situation sociale, aux parcours administratifs, aux données biométriques ou encore aux informations stratégiques détenues par les organismes publics. L'atteinte à ces données peut compromettre non seulement les droits fondamentaux des citoyens, notamment le droit à la vie privée et à la protection des données personnelles, mais également la continuité du service public, la sécurité des systèmes d'information et la confiance des usagers dans les institutions publiques.

Dans ce contexte, le secteur public marocain se trouve placé devant une exigence renouvelée : il ne s'agit plus uniquement de collecter, conserver ou exploiter les données nécessaires à l'action administrative, mais de les gouverner juridiquement. La gouvernance juridique des données sensibles renvoie ainsi à l'ensemble coordonné des règles, responsabilités, procédures, contrôles et mécanismes de redevabilité permettant d'assurer la conformité des traitements, la sécurité des systèmes, la protection des personnes concernées et la maîtrise des risques tout au long du cycle de vie de la donnée, depuis sa collecte jusqu'à sa destruction ou son archivage. Elle suppose une organisation interne claire, une qualification rigoureuse des données, une documentation des traitements, un encadrement des prestataires, une traçabilité des opérations et une capacité effective de contrôle.

Le droit marocain offre, à cet égard, un socle normatif et institutionnel significatif. La loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue le cadre général de protection des personnes concernées. Elle

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

organise les conditions de licéité des traitements, les droits des individus, les obligations des responsables de traitement, ainsi que le rôle de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. À ce premier pilier s'ajoute la loi n° 05-20 relative à la cybersécurité, qui renforce la protection des systèmes d'information, notamment ceux des entités publiques et des infrastructures d'importance vitale, en consacrant des exigences de sécurité, de résilience et de prévention des incidents. Plus récemment, l'encadrement du recours aux prestataires de services cloud par certaines entités manipulant des systèmes d'information ou des données sensibles confirme que la gouvernance des données publiques ne peut plus être séparée des enjeux de souveraineté numérique, de dépendance technologique et de maîtrise contractuelle des infrastructures d'hébergement.

Les notions mobilisées dans cette étude doivent être précisées. Les données sensibles seront entendues dans une acception à la fois juridique et fonctionnelle. Elles renvoient non seulement aux données expressément qualifiées comme sensibles par le droit de la protection des données personnelles, telles que les données de santé, les données biométriques, les opinions ou les convictions, mais aussi, plus largement, à toute donnée dont l'atteinte peut produire un risque élevé pour les droits et libertés des personnes ou pour l'intérêt public. Sont donc concernées les données sociales, judiciaires, administratives, identifiantes, stratégiques ou critiques au regard des missions exercées par les organismes publics. Les technologies émergentes désignent, quant à elles, les outils et systèmes qui transforment les chaînes de traitement, de circulation et de décision, notamment l'intelligence artificielle, le Big Data, le cloud computing, l'Internet des objets, les systèmes biométriques, la blockchain ou encore les dispositifs de smart city. Enfin, le secteur public marocain sera entendu comme englobant les administrations de l'État, les collectivités territoriales, les établissements et entreprises publics, ainsi que les entités publiques ou assimilées opérant des systèmes d'information sensibles ou soumises à des exigences renforcées en matière de cybersécurité.

La présente recherche porte donc sur la gouvernance juridique des données sensibles dans le secteur public marocain à l'épreuve des technologies émergentes. Son objectif principal est d'analyser la capacité du cadre juridique marocain, notamment la loi n° 09-08 relative à la protection des données à caractère personnel, la loi n° 05-20 relative à la cybersécurité et les règles relatives au recours aux services cloud, à encadrer efficacement les traitements de données sensibles opérés par les administrations publiques. Elle vise également à montrer que l'effectivité de cette gouvernance dépend non seulement de l'existence de normes juridiques,

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

mais aussi de leur traduction en mécanismes organisationnels, procéduraux et contractuels de conformité, de contrôle et de redevabilité.

L'intérêt de cette étude est triple. Sur le plan scientifique, elle permet d'articuler des branches du droit souvent analysées séparément : protection des données personnelles, cybersécurité, droit administratif, responsabilité publique, souveraineté numérique et régulation des technologies émergentes. Sur le plan pratique, elle propose une lecture opérationnelle de la conformité, fondée sur la clarification des rôles, la cartographie des traitements, la classification des données, les procédures internes, les audits, les contrats et la gestion des risques. Sur le plan institutionnel, elle met en lumière la nécessaire coordination entre les obligations de protection des personnes, portées notamment par la loi n° 09-08 et la CNDP, et les obligations de sécurité et de résilience des systèmes d'information, renforcées par la loi n° 05-20 et les textes associés. Dès lors, la question centrale n'est plus seulement celle de la conformité formelle aux textes applicables. Elle est celle de la capacité des institutions publiques à transformer ce cadre normatif en pratiques effectives, vérifiables et traçables. Autrement dit, il ne suffit pas que les administrations soient juridiquement tenues de protéger les données sensibles ; encore faut-il qu'elles puissent démontrer, par des mécanismes de gouvernance, qu'elles maîtrisent les finalités des traitements, les risques de sécurité, les interventions des prestataires, les flux inter-administratifs et les effets des technologies utilisées.

La problématique peut donc être formulée ainsi : dans quelle mesure le cadre juridique marocain, fondé sur la protection des données personnelles, la cybersécurité et l'encadrement du cloud, permet-il d'assurer une gouvernance effective des données sensibles dans le secteur public face aux technologies émergentes, et quelles exigences organisationnelles, procédurales et contractuelles doivent être renforcées pour transformer ce cadre en pratiques opérationnelles de conformité et de redevabilité ?

L'hypothèse défendue est que le régime marocain offre des fondations normatives pertinentes pour encadrer la gouvernance des données sensibles dans le secteur public, mais que son efficacité dépend principalement de sa traduction organisationnelle. La difficulté majeure ne réside pas nécessairement dans l'absence de règles, mais dans la capacité des administrations à structurer des dispositifs internes de gouvernance : cartographie des traitements, classification des données, documentation, analyses d'impact, audits, contractualisation des prestataires, traçabilité des accès et contrôle continu des systèmes. Les technologies émergentes déplacent ainsi le centre de gravité du risque : l'opacité algorithmique, la dépendance au cloud,

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

l'interconnexion des bases de données, l'usage de la biométrie ou les dispositifs IoT imposent une gouvernance orientée vers la preuve, la responsabilité et l'auditabilité.

Sur le plan méthodologique, cette recherche s'inscrit dans une approche juridique qualitative, de nature analytique et normative. Elle repose sur l'analyse des textes législatifs et réglementaires marocains applicables à la protection des données personnelles, à la cybersécurité, à l'accès à l'information, à l'archivage public et à l'encadrement du cloud. Le positionnement retenu est principalement positiviste et interprétatif : il s'agit, d'une part, d'examiner le contenu des normes en vigueur et, d'autre part, d'en apprécier la portée pratique face aux risques générés par les technologies émergentes. Le raisonnement adopté est essentiellement déductif, dans la mesure où l'étude part du cadre juridique existant pour en évaluer l'application aux situations nouvelles liées à l'intelligence artificielle, au Big Data, à l'interopérabilité, à la biométrie et aux services cloud. Cette démarche est complétée par une lecture fonctionnelle de la gouvernance des données, permettant de relier les exigences juridiques aux mécanismes opérationnels de conformité, de contrôle, d'audit et de redevabilité.

Pour vérifier cette hypothèse, l'étude sera organisée autour de deux axes complémentaires. La première partie sera consacrée aux fondations juridiques et institutionnelles de la gouvernance des données sensibles dans le secteur public marocain. Elle analysera, d'une part, la qualification juridique des données sensibles et les principes directeurs du traitement, et, d'autre part, la sécurisation normative issue de la cybersécurité, de la protection des infrastructures critiques et de l'encadrement du cloud. La seconde partie portera sur l'opérationnalisation de cette gouvernance face aux technologies émergentes. Elle examinera d'abord les mécanismes organisationnels de conformité et de redevabilité, avant d'étudier la gouvernance par le risque technologique, notamment à travers l'intelligence artificielle, l'interconnexion des systèmes, l'IoT, la biométrie et les dispositifs publics intelligents.

1. Les fondations juridiques et institutionnelles de la gouvernance des données sensibles dans le secteur public marocain

Dans le secteur public marocain, la gouvernance des données sensibles s'inscrit au croisement de plusieurs exigences juridiques : la protection des personnes concernées, la continuité et la qualité du service public, la sécurité des systèmes d'information, ainsi que les impératifs de transparence administrative et de conservation patrimoniale. Ce champ se structure autour d'un noyau de règles générales fixées par la loi n° 09-08 relative à la protection des personnes

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

physiques à l'égard du traitement des données à caractère personnel[1], complétées par des normes sectorielles et transversales applicables aux administrations (droit d'accès à l'information, règles d'archivage public, conditions de sous-traitance et de transferts internationaux).

L'enjeu central est d'ordonner, dans une logique de proportionnalité, la circulation de l'information entre administrations (interopérabilité, mutualisation, dispositifs de partage) sans fragiliser les droits fondamentaux des citoyens, notamment lorsque les traitements portent sur des données « sensibles » au sens strict (santé, opinions, convictions) ou sur des données dont l'usage public peut générer un risque élevé d'atteinte à la vie privée.

1.1 La qualification juridique des données sensibles et les principes directeurs du traitement

La qualification juridique des données dites « sensibles » constitue la première étape d'une gouvernance conforme, car elle déclenche un régime renforcé de licéité, d'autorisation et de sécurité.

Dans l'architecture de la loi n° 09-08, cette qualification n'est pas seulement une catégorie descriptive : elle organise un niveau supérieur de contrôle ex ante (autorisation) et impose une vigilance accrue quant à la finalité, à la minimisation, à l'information des personnes, à la traçabilité des accès et aux conditions de conservation. Pour les autorités publiques, l'enjeu est double : (i) assurer que les traitements sensibles sont strictement arrimés à une mission d'intérêt général ou à un fondement légal/statutaire ; (ii) documenter la conformité de bout en bout (procédures internes, clauses contractuelles de sous-traitance, mesures techniques et organisationnelles, audits) afin de répondre aux exigences de la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) et, plus largement, aux obligations de bonne administration[2].

1.1.1 Notion de donnée personnelle et logique de protection des personnes (loi 09-08, CNDP)

Le droit marocain appréhende la donnée personnelle à travers une logique de protection de la personne concernée, entendue comme titulaire de droits opposables au responsable du traitement, y compris lorsqu'il s'agit d'une autorité publique.

[1] Loi n° 09-08, art. 1 (définitions, dont « données sensibles ») et art. 4 à 11 (droits des personnes), Dahir n° 1-09-15 du 18 février 2009 ; CNDP, texte consolidé de la loi 09-08 (version publiée en 2023).
[2] Loi n° 09-08, art. 1 (définition des données sensibles), art. 21 (régime d'autorisation), art. 24 (mesures de sécurité), art. 27-28 (pouvoirs/attributions CNDP) ; CNDP, « Loi 09-08 » (page officielle) et PDF de la loi (2023).

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

La loi n° 09-08[3] définit les « données à caractère personnel » comme toute information, quelle que soit sa nature et indépendamment de son support, relative à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant ou à un ou plusieurs éléments spécifiques propres à son identité. Dans cette perspective, la protection ne vise pas le secret en soi, mais la prévention des usages abusifs susceptibles de porter atteinte à l'identité, aux libertés et aux droits, en particulier lorsque les traitements deviennent massifs, interconnectés ou automatisés.

En effet, la loi formalise cette logique au moyen de principes directeurs : détermination préalable et légitime des finalités, pertinence et non-excessivité des données, exactitude et mise à jour, limitation de la durée de conservation, sécurité et confidentialité, et information loyale des personnes lors de la collecte.

Le corollaire institutionnel est le rôle de la CNDP (Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel)[4], instituée auprès du Chef du Gouvernement, dont la mission est de veiller au respect de la loi, d'émettre des avis sur les projets de textes relatifs aux traitements, de recevoir déclarations/notifications et, surtout, d'autoriser ou d'encadrer les traitements à risques, notamment ceux portant sur des données sensibles ou de santé.

Sur le plan des droits, la personne concernée dispose notamment de droits d'information, d'accès, de rectification et d'opposition, ce qui oblige l'administration à concevoir des parcours d'exercice des droits compatibles avec ses contraintes opérationnelles (identification, authentification, délais, traçabilité) tout en respectant les exceptions prévues, par exemple pour la défense nationale, la sûreté ou la prévention/répression du crime.

1.1.2 Spécificités du secteur public

Dans le secteur public, la gouvernance des données sensibles se caractérise par une tension structurante entre la finalité d'intérêt général et la protection des droits individuels.

D'une part, l'administration traite des données pour délivrer des prestations, instruire des demandes, exercer des prérogatives de puissance publique ou organiser des politiques publiques ; ces traitements peuvent reposer sur une base légale ou statutaire et s'inscrire dans des chaînes de valeur administratives impliquant plusieurs organismes (partage, interconnexion, mutualisation). D'autre part, l'intensification du « partage inter-administrations » accroît le

[3] Loi n° 09-08, art. 1 (définitions), art. 5-6 (information), art. 7-9 (accès, rectification, opposition), art. 6 (exceptions), art. 27 (institution de la CNDP).
[4] CNDP, « Loi 09-08 » (site officiel) : Commission nationale de contrôle de la protection des données à caractère personnel

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

risque d'extension de finalité et d'opacité : la gouvernance exige alors une cartographie des flux, une définition claire des rôles (responsable de traitement, co-responsables, sous-traitants), des règles de minimisation et de cloisonnement, et des mécanismes de contrôle (journaux d'accès, habilitations, audits).

En matière de conservation, l'administration ne peut se limiter à une logique de « suppression » au terme d'un usage opérationnel : elle doit articuler la limitation de durée posée par la loi 09-08[5] avec les obligations d'archivage public, lesquelles organisent, dans l'intérêt public, la constitution, la gestion, le tri et le versement des archives[6] (archives courantes, intermédiaires, définitives) afin de justifier des droits, assurer la continuité administrative et préserver le patrimoine national.

Cette articulation est également influencée par le droit d'accès à l'information (loi n° 31-13[7]), qui consacre un principe de transparence de l'action administrative (sur fondement constitutionnel)[8], tout en admettant des limites tenantes, notamment, à la protection de la vie privée et des données personnelles : la gouvernance doit ainsi intégrer des procédures de communication partielle (occultation/anonymisation) et de gestion des demandes, sans créer de « fuites » de données sensibles.

Enfin, la dimension « externe » de la gouvernance concerne les transferts et l'externalisation : le transfert de données vers un État étranger est soumis, en principe, à l'existence d'un niveau de protection suffisant et à un encadrement par la CNDP, avec des dérogations strictes (consentement exprès, intérêt public, entraide judiciaire, etc.).

De même, la sous-traitance publique des traitements impose une contractualisation explicite des instructions, des obligations de confidentialité et des mesures de sécurité, afin de maintenir la maîtrise par l'administration et d'assurer la responsabilité du traitement tout au long de la chaîne, ce qui est particulièrement critique pour les données sensibles ou de santé.

1.2 La sécurisation normative : cybersécurité, infrastructures critiques et encadrement du cloud

La protection des données sensibles dans le secteur public ne relève plus uniquement de la technique : elle constitue un enjeu juridique et stratégique. La numérisation des services publics, l'usage croissant de plateformes partagées et la montée en puissance des prestataires cloud ont

[5] Loi n° 09-08, art. 24-26 (sécurité, secret professionnel, sous-traitance), art. 43-44 (transferts internationaux), art. 21 (données sensibles).
[6] Loi n° 69-99 relative aux archives, art. 1-5 (définition/gestion des archives publiques).
[7] Loi n° 31-13 relative au droit d'accès à l'information, Dahir du 22 février 2018 (publication au Bulletin officiel), art. 1 (champ/objectif).
[8] Constitution du Royaume du Maroc, art. 27 (droit d'accès à l'information).

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

transformé la nature des risques et déplacé le centre de gravité de la gouvernance vers des réponses normatives et institutionnelles. Ce chapitre examine d'abord l'assise normative de la cybersécurité[9] applicable aux systèmes d'information publics et aux infrastructures critiques, puis analyse le traitement réglementaire du recours au cloud en tant que vecteur de dépendance et de souveraineté numérique[10].

1.2.1 Portée de la loi 05-20 et obligations de sécurité/résilience pour les entités publiques et SI sensibles

La protection des données sensibles détenues par les administrations publiques s'inscrit aujourd'hui dans un cadre normatif qui impose des obligations juridiques positives de sécurisation des systèmes d'information, fondées sur la mise en œuvre de mesures techniques, organisationnelles et procédurales destinées à prévenir les intrusions, détecter les anomalies et réagir efficacement aux incidents. Ces obligations traduisent une combinaison d'exigences de moyens et de résultats : les entités publiques sont tenues d'adopter des dispositifs proportionnés au niveau de sensibilité des informations traitées, tout en garantissant la disponibilité, l'intégrité et la confidentialité des données dans des conditions normales comme en situation de crise. Cette approche dépasse la logique traditionnelle de conformité réglementaire pour consacrer une véritable exigence de résilience opérationnelle, entendue comme la capacité des institutions publiques à maintenir ou à rétablir la continuité des services essentiels malgré la survenance d'événements perturbateurs, qu'ils soient d'origine technique, humaine ou malveillante. Dans cette architecture, les infrastructures qualifiées d'importance vitale occupent une place particulière, justifiant un régime juridique différencié caractérisé par des obligations renforcées d'audit, de surveillance permanente, de planification de continuité d'activité et de coopération institutionnelle avec les autorités nationales spécialisées en cybersécurité, afin d'assurer une gestion coordonnée des crises numériques susceptibles d'affecter l'intérêt général.

Toutefois, l'effectivité de ce dispositif se heurte aux transformations structurelles induites par la digitalisation de l'action publique, notamment l'externalisation croissante des services informatiques vers des prestataires technologiques, qui introduit de nouvelles zones d'incertitude quant à la répartition des responsabilités, à la transparence des infrastructures d'hébergement et à la maîtrise des chaînes de traitement des données. Cette dépendance technique soulève des interrogations juridiques majeures relatives à l'opposabilité des obligations de sécurité aux prestataires externes, à l'accès aux mécanismes de contrôle et

[9] Koops, B. J. (2019). Cybersecurity regulation in the EU: The NIS Directive and beyond. Springer.
[10] Bensamoun, A., & Loiseau, G. (2021). Droit du numérique : Contrats, innovation, données et gouvernance. Eyrolles.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

d'audit, ainsi qu'à la capacité des administrations à garantir la souveraineté opérationnelle de leurs systèmes.

Dès lors, la réglementation existante, principalement conçue pour encadrer des systèmes internalisés, révèle ses limites face aux modèles d'externalisation numérique, ce qui appelle une évolution du cadre normatif vers un encadrement plus précis des relations contractuelles avec les prestataires, l'instauration d'exigences de transparence et de traçabilité renforcées, ainsi que la mise en place de mécanismes de vérification indépendante, afin de transformer les impératifs techniques de cybersécurité en responsabilités juridiques effectives et opposables dans la gouvernance des données publiques sensibles.

1.2.2 Le cloud comme enjeu de gouvernance : conditions de recours et maîtrise des dépendances (décret cloud)

Le recours aux services cloud[11] par les administrations publiques constitue une transformation profonde des modes de gestion des systèmes d'information, offrant des gains significatifs en flexibilité opérationnelle, en mutualisation des ressources et en optimisation des coûts, tout en transférant une partie du contrôle technique vers des prestataires externes. Cette externalisation redessine les chaînes de traitement des données publiques et expose les pouvoirs publics à des risques stratégiques liés, d'une part, à la perte de maîtrise directe sur les infrastructures d'hébergement et, d'autre part, à la dépendance croissante envers des fournisseurs technologiquement dominants. Sur le plan juridique, cette situation soulève des enjeux relatifs à la répartition des responsabilités entre administrations et prestataires, à l'accès effectif aux journaux d'activité nécessaires au contrôle et à l'audit, ainsi qu'à la localisation des données et aux garanties offertes aux personnes concernées quant à la transparence des traitements opérés[12].

Face à ces défis, l'instauration de mécanismes de qualification ou d'agrément des prestataires cloud apparaît comme une réponse structurante, permettant de subordonner le recours à ces services à des critères de fiabilité technique, de sécurité organisationnelle et de conformité juridique, tout en imposant des exigences renforcées de transparence, d'auditabilité et de traçabilité des opérations. Ce type de dispositif modifie la nature de la relation entre l'administration et le prestataire, en introduisant une dimension de contrôle public préalable qui dépasse la simple logique contractuelle et renforce la responsabilité des autorités publiques dans le choix et la supervision des fournisseurs.

[11] ANSSI. (2019). Sec Num Cloud: Référentiel de sécurité pour les services cloud. Agence nationale de la sécurité des systèmes d'information.
[12] Millard, C. (Ed.). (2013). Cloud computing law. Oxford University Press.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

Toutefois, la sécurisation du recours au cloud ne saurait se limiter à la sélection des prestataires ; elle implique également l'intégration d'exigences de réversibilité, d'interopérabilité et de portabilité des données dans les relations contractuelles, afin de prévenir les phénomènes d'enfermement technologique et de garantir la capacité des administrations à reprendre la maîtrise de leurs systèmes en cas de défaillance ou de changement de stratégie. Ces exigences, qu'elles soient imposées directement par la réglementation ou indirectement par des schémas de certification et de normalisation, traduisent une volonté de préserver l'autonomie opérationnelle des pouvoirs publics.

Enfin, cette dynamique de gouvernance du cloud s'inscrit dans une tension permanente entre souveraineté numérique et coopération internationale, car la maîtrise nationale des données sensibles ne peut s'affranchir des standards techniques mondiaux ni des mécanismes de reconnaissance mutuelle entre autorités de contrôle ; elle suppose au contraire la construction d'un niveau de confiance partagé permettant d'accepter certaines externalisations transfrontalières tout en réservant les traitements critiques à des environnements soumis à une souveraineté renforcée[13].

2. L'opérationnalisation de la gouvernance juridique face aux technologies émergentes (modèle de conformité et de redevabilité)

L'opérationnalisation de la gouvernance juridique des données sensibles, face aux technologies émergentes, repose sur une organisation institutionnelle et normative rigoureuse, fondée sur des mécanismes efficaces de conformité et de redevabilité. Elle implique l'adoption de cadres réglementaires adaptés, la clarification des responsabilités des acteurs publics et la mise en place de dispositifs de contrôle, d'audit et d'évaluation, destinés à garantir la légalité, la transparence et la sécurité des traitements de données. Dans ce contexte, l'instauration de modèles de gouvernance intégrés permet de concilier innovation technologique et protection des droits fondamentaux, tout en assurant la confiance des citoyens et la crédibilité de l'action publique.

2.1 Gouverner par l'organisation : rôles, procédures, preuves de conformité

Dans l'ordre juridique marocain, la protection des données à caractère personnel s'inscrit d'abord dans un socle constitutionnel : l'article 24 consacre le droit à la protection de la vie privée. Ce principe irrigue ensuite un régime spécialisé, porté par la loi n° 09-08[14], qui encadre

[13] ENISA. (2021). Cloud security: Recommendations and good practices. European Union Agency for Cybersecurity.
[14] Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Bulletin Officiel, Rabat, 2009.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

les traitements automatisés ou non, crée des obligations de fond (finalité déterminée, proportionnalité, sécurité, limitation de conservation, droits des personnes) et des obligations procédurales (déclaration/autorisation, encadrement des transferts, contrôle).

L'essor des technologies émergentes transforme cependant la nature des risques juridiques. L'IA et l'analytique peuvent produire des décisions ou des recommandations impactant directement les administrés (accès à un droit, contrôle, ciblage), tandis que la biométrie et l'interconnexion de fichiers amplifient les risques de surveillance ou de détournement de finalité. Le cloud et l'externalisation reconfigurent la chaîne de responsabilité et la souveraineté des données. Dès lors, une gouvernance juridiquement pertinente doit répondre à une double exigence: (1) respecter les conditions de licéité et de protection posées par le droit, et (2) démontrer, par des preuves, l'effectivité de ce respect (accountability).

Dans le secteur public, l'exigence de preuve s'articule aussi avec la transparence de l'action administrative : la loi n° 31-13[15] sur le droit d'accès à l'information renforce l'impératif de traçabilité, de justification et de documentation des décisions, tout en imposant de concilier transparence et protection des données. Enfin, la loi n° 05-20 sur la cybersécurité renforce la dimension normative de la sécurité des systèmes d'information publics (règles, mesures, directives et référentiels), ce qui rend indissociables la conformité « données » et la conformité « sécurité ».

2.1.1 Architecture de gouvernance : responsable de traitement, sous-traitants, comités, référentiels internes, classification des données, registre et documentation

L'architecture de gouvernance est le dispositif juridique d'imputation. Elle transforme des obligations générales en responsabilités assignées et en circuits de décision opposables. En droit, la question centrale est : qui répond du traitement ? La loi n° 09-08 place la charge principale sur le responsable du traitement, c'est-à-dire l'entité qui détermine les finalités et moyens. Dans l'administration, cela implique de désigner explicitement l'autorité compétente (ministère, établissement public, collectivité) et d'identifier les unités qui déterminent effectivement les choix (direction métier, DSI, direction des systèmes d'information, prestataire). Le risque, dans les projets émergents, est le glissement de responsabilité vers un prestataire « concepteur » (éditeur IA, intégrateur cloud) sans maîtrise suffisante par l'administration. Or, juridiquement, l'externalisation ne neutralise pas les obligations : elle exige un encadrement contractuel, des contrôles et une capacité d'audit.

[15] Loi n° 31-13 relative au droit d'accès à l'information. Bulletin Officiel, Rabat, 2018.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

La qualification du sous-traitant doit donc être documentée et articulée à des clauses de conformité (confidentialité, sécurité, limitation de finalité, sous-traitance ultérieure, localisation/accès, réversibilité et destruction). Pour le secteur public, cette exigence rejoint la logique de commande publique : les cahiers des charges et conventions doivent intégrer des obligations probatoires (rapports, journaux, droit d'audit, délais de notification). Cette contractualisation est un outil de gouvernance juridique : elle permet de rendre opposables les obligations de sécurité et de traçabilité, donc de produire la preuve de conformité.

L'instauration de comités et de référents n'est pas un simple choix managérial : c'est une condition de légalité en contexte de risques élevés. Un comité de gouvernance des données permet de vérifier la conformité des finalités (intérêt public, nécessité), l'adéquation des données (minimisation), et la compatibilité des nouveaux usages. Un référent « protection des données » coordonne la documentation (registre, dossiers), l'information des personnes, la gestion des demandes et la conformité aux procédures CNDP[16]. Un référent « cybersécurité » assure la cohérence avec les exigences de la loi 05-20[17] et les référentiels techniques (homologation, gestion des vulnérabilités, continuité).

La classification des données est, d'un point de vue juridique, l'outil qui fait passer de l'abstraction (données personnelles / données sensibles) à un régime de traitement différencié. La CNDP[18] rappelle que certains traitements requièrent une autorisation préalable, notamment lorsqu'ils portent sur des données sensibles (santé, opinions, etc.), sur des données d'infractions/condamnations, sur l'interconnexion de fichiers gérant un service public avec des finalités d'intérêt public différentes, ou encore sur certains identifiants.

Une classification rigoureuse doit donc intégrer : la catégorie juridique de la donnée, la finalité, et le scénario d'usage technologique (interconnexion, IA, biométrie, cloud). Cela permet de déclencher, en amont, le bon régime procédural (déclaration vs autorisation, demandes CNDP, garanties supplémentaires) et les mesures de sécurité proportionnées.

Le registre et la documentation constituent enfin l'ossature probatoire. Au-delà de l'inventaire, ils matérialisent la conformité : finalité, base de mise en œuvre, catégories de données, destinataires, durées, mesures de sécurité, transferts, et justification de la

[16] Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP), Délibération n° D-188-2020 du 14 décembre 2020 relative à l'analyse d'impact sur la protection des données (AIPD). Rabat, 2020.
[17] Loi n° 05-20 relative à la cybersécurité. Bulletin Officiel, Rabat, 2020.
[18] Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). Procédures de notification : déclaration, autorisation préalable et transfert de données à caractère personnel à l'étranger. Rabat.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

nécessité/proportionnalité. Dans une approche juridique exigeante, chaque traitement à fort impact doit disposer d'un dossier de conformité, notamment lorsque le traitement relève de l'autorisation préalable (données sensibles, biométrie, interconnexion) : pièces CNDP, analyses de risques, contrats, politiques applicables, preuves d'information, et preuves techniques. L'administration peut alors démontrer, de manière structurée, sa diligence et sa maîtrise.

2.1.2 Gouverner par le contrôle : analyses d'impact/évaluation des risques, audits, gestion des incidents, traçabilité et exigence de "preuve"

Gouverner par le contrôle revient à instaurer une boucle juridique d'effectivité : vérifier que les obligations sont réellement respectées dans le temps, et corriger. Dans les technologies émergentes, la conformité est dynamique (évolution des jeux de données, des modèles IA, des paramétrages, des prestataires). Ainsi, le contrôle n'est pas un supplément : c'est la condition de la redevabilité. Il s'organise autour de l'évaluation ex ante (analyses d'impact/risques), de la vérification ex post (audit), de la réaction (incidents) et de la preuve (traçabilité).

Les analyses d'impact et l'évaluation des risques ont une fonction juridique précise : démontrer la nécessité et la proportionnalité, et réduire le risque d'atteinte aux droits. La CNDP a encadré l'analyse d'impact relative à la protection des données (AIPD) comme un processus visant à décrire le traitement, apprécier sa nécessité/proportionnalité, identifier les risques pour les droits et libertés et déterminer les mesures de mitigation. Dans l'administration, cette analyse doit être exigée, a minima, pour les traitements sensibles et ceux mobilisant l'IA décisionnelle, la biométrie ou l'interconnexion de bases, car ces usages concentrent les risques de discrimination, d'erreur et de détournement de finalité. Elle guide également la qualification du régime CNDP (autorisation préalable, pièces à produire) et l'architecture de sécurité.

L'audit, sur le plan juridique, vise à objectiver l'effectivité des garanties promises : contrôle des habilitations, justification des accès, application des durées de conservation, sécurisation des environnements, et conformité contractuelle des sous-traitants. Pour l'IA, l'audit doit inclure des éléments propres au risque algorithmique : gouvernance des données d'entraînement, documentation des modèles, traçabilité des versions, détection de dérive et mécanismes de supervision humaine. Les cadres internationaux (OCDE[19], NIST) renforcent cette approche en insistant sur l'imputabilité tout au long du cycle de vie et sur la robustesse des systèmes.

[19] Organisation de Coopération et de Développement Économiques (OCDE). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Paris, 2019.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

La gestion des incidents est un volet essentiel de la redevabilité : un incident révèle non seulement une faiblesse technique, mais aussi la capacité de l'organisation à qualifier, contenir, documenter et corriger. La loi 05-20 promeut un cadre de règles et mesures de sécurité visant la résilience des systèmes d'information des administrations et des entités publiques, ce qui implique une préparation : plans, responsabilités, procédures d'escalade, continuité et preuves (journaux, rapports, décisions). Dans une perspective CNDP, la qualité de la documentation après incident (données touchées, temporalité, destinataires, mesures prises) conditionne la crédibilité de la conformité et la maîtrise du risque contentieux ou disciplinaire.

La traçabilité et l'exigence de preuve constituent le noyau de l'accountability. Une administration doit pouvoir démontrer : (1) que les accès et traitements sont autorisés, (2) que les incidents sont détectés et gérés, et (3) que les sous-traitants respectent les clauses. Concrètement, cela requiert des journaux d'accès et d'administration, des traces d'export et d'interconnexion, des registres de décisions des comités, des rapports d'audit, et la conservation de versions (données/modèles) lorsque l'IA intervient. Cette preuve n'a pas seulement une fonction de contrôle externe : elle protège l'administration en établissant la diligence, la proportionnalité des mesures et la capacité à corriger. À l'échelle internationale, l'adhésion du Maroc à la Convention 108 renforce l'inscription de cette logique probatoire dans un cadre de protection des données à vocation transfrontière[20].

2.2 Gouverner par le risque technologique : IA, interconnexion, biométrie, smart city

La transformation numérique de l'action publique s'accompagne d'une montée en puissance des risques technologiques liés à l'usage de l'intelligence artificielle, à l'interconnexion des systèmes et au déploiement de dispositifs biométriques et urbains intelligents. Ces évolutions imposent un renouvellement des modes de régulation, désormais orientés vers une approche préventive et intégrée fondée sur la gestion des risques. Dans ce contexte, la gouvernance publique est appelée à concilier innovation technologique, efficacité administrative et protection des droits fondamentaux. Le présent chapitre examine, à cet égard, les exigences croissantes de gouvernance algorithmique (A) ainsi que la nécessité d'une régulation intégrée des systèmes interconnectés (B).

[20] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Strasbourg, 1981. Adhésion du Maroc, 2019.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

2.2.1 IA dans l'action publique : transparence, explicabilité, non-discrimination, maîtrise des jeux de données, encadrement des prestataires

Le recours croissant à l'intelligence artificielle dans l'action publique[21] s'inscrit dans un mouvement mondial de transformation numérique de l'État, auquel le Maroc prend pleinement part à travers ses politiques de digitalisation et de modernisation administrative. Qu'il s'agisse de la gestion des services publics, de la fiscalité ou de la sécurité, les systèmes algorithmiques participent désormais aux processus décisionnels de l'administration, redessinant en profondeur les modes d'intervention de la puissance publique.

Dans ce contexte, la notion de gouvernance algorithmique[22] s'affirme comme un cadre structurant, destiné à encadrer l'usage de ces technologies dans le respect des principes fondamentaux de l'État de droit. Au Maroc, cette gouvernance repose sur un socle juridique et institutionnel en cours de consolidation, articulé notamment autour de la loi n° 09-08 1relative à la protection des données à caractère personnel et du rôle de la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP).

En premier lieu, l'exigence de transparence et d'explicabilité des décisions algorithmiques[23] trouve un ancrage solide dans le droit marocain de la protection des données. La loi n° 09-08 reconnaît en effet le droit à l'information des personnes concernées lors de la collecte et du traitement de leurs données, imposant aux administrations publiques d'informer les usagers du recours à des traitements automatisés. Cette exigence, renforcée par les missions de contrôle et d'accompagnement de la CNDP, contribue à l'émergence d'une culture de transparence dans l'usage des technologies numériques.

En deuxième lieu, la question des biais algorithmiques et du respect du principe d'égalité s'inscrit dans le prolongement des garanties constitutionnelles et légales marocaines. Si la loi n° 09-08 n'aborde pas explicitement la problématique des biais algorithmiques, elle impose néanmoins des obligations de loyauté et de licéité dans le traitement des données, susceptibles d'engager la responsabilité de l'administration en cas de discrimination indirecte résultant d'un traitement automatisé. Face à l'essor de l'intelligence artificielle, cette exigence appelle un renforcement des mécanismes d'audit et de contrôle des systèmes algorithmiques déployés par les pouvoirs publics.

[21] Rose Pola Pricemou & Michel Boukar, Intelligence artificielle et e-gouvernance en Afrique : vers une administration publique transparente et plus efficace, L'Harmattan, 2025.
[22] Bellan, C. (2022). La gouvernance algorithmique et la transformation de l'action publique. Paris : L'Harmattan.
[23] Zerilli, J., Knott, A., Maclaurin, J., & Gavaghan, C. (2019). Transparency in Algorithmic and Human Decision-Making: Is There a Double Standard? Philosophy & Technology, 32(4), 661–683.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

En troisième lieu, la gouvernance des données constitue un pilier fondamental de la régulation de l'intelligence artificielle au Maroc. La loi n° 09-08 soumet les responsables de traitement à des obligations strictes en matière de sécurité, de finalité et de proportionnalité des données collectées. La CNDP, en tant qu'autorité de régulation, joue un rôle central dans le contrôle des traitements, notamment à travers les mécanismes de déclaration, d'autorisation préalable et de sanction en cas de manquement[3]. Cette architecture normative contribue à façonner un modèle marocain de gouvernance des données, appelé à évoluer face aux défis posés par l'IA et la circulation internationale des données.

En quatrième lieu, l'intégration de l'intelligence artificielle dans l'action publique s'inscrit dans une stratégie nationale plus ambitieuse de transformation digitale. À cet égard, des initiatives telles que la stratégie « Maroc Digital 2030[24] » visent à positionner le Royaume comme un acteur régional de premier plan dans le domaine du numérique, en développant les infrastructures, les compétences et l'innovation technologique[4]. Cette orientation stratégique renforce la nécessité d'un encadrement juridique adapté, en mesure d'accompagner le déploiement des systèmes d'IA dans le respect des exigences de souveraineté numérique et de protection des droits fondamentaux.

Enfin, l'exigence de performance des systèmes d'intelligence artificielle s'impose comme un complément indispensable à la légalité. Dans le contexte marocain, la conformité à la loi n° 09-08 apparaît elle-même comme un vecteur de confiance et de performance organisationnelle, en favorisant la qualité des données, la sécurisation des traitements et l'efficacité des processus décisionnels[5]. La gouvernance algorithmique ne saurait dès lors se réduire à une logique formelle de conformité : elle implique une articulation étroite entre efficacité technologique, sécurité juridique et acceptabilité sociale.

Ainsi, l'intégration de l'intelligence artificielle dans l'action publique marocaine appelle une reconfiguration en profondeur des cadres de gouvernance, à la croisée du droit, de la technologie et des politiques publiques. L'enjeu n'est pas tant celui de l'adoption des outils que celui de leur maîtrise, dans une perspective de confiance, de souveraineté et de protection effective des droits des citoyens.

[24] Ministère de la Transition numérique et de la Réforme de l'administration. (2024). Stratégie Maroc Digital 2030 : Plaquette institutionnelle. Rabat.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

2.2.2 Interopérabilité, IoT et biométrie : vers une régulation intégrée des systèmes interconnectés

L'intégration croissante de l'interopérabilité, de l'Internet des objets (IoT) et des technologies biométriques dans les systèmes publics contemporains conduit à l'émergence d'une régulation juridique de plus en plus structurée, orientée vers la mise en place d'un cadre normatif intégré[25]. L'interopérabilité, en tant que principe technique et juridique, permet d'assurer la circulation fluide, sécurisée et standardisée des données entre administrations et systèmes hétérogènes, constituant ainsi un levier essentiel de modernisation de l'action publique et de continuité des services numériques. Toutefois, l'extension des dispositifs IoT, caractérisés par une interconnexion massive d'objets collectant et transmettant des données en temps réel, ainsi que le recours croissant aux technologies biométriques dans les processus d'identification et d'authentification, soulèvent des enjeux juridiques majeurs relatifs à la protection des données personnelles, à la sécurité des systèmes d'information et à la souveraineté numérique de l'État. Dans ce contexte, la régulation ne peut plus être fragmentée, mais doit s'inscrire dans une approche systémique et cohérente, fondée sur des exigences renforcées de standardisation, de certification des dispositifs et de gouvernance des flux de données[26]. Cette dynamique implique également l'encadrement strict des traitements biométriques, en raison de leur sensibilité particulière, ainsi que l'adoption de mécanismes de contrôle et d'audit permettant de garantir la conformité des systèmes interconnectés aux principes fondamentaux du droit numérique, notamment la transparence, la sécurité, la minimisation des données et la responsabilité des acteurs publics et privés impliqués[27].

[25] BENABDELLAH, Mohammed Amine. Droit du numérique et transformation digitale de l'administration publique au Maroc. Casablanca : Éditions La Croisée des Chemins, 2023.
[26] OCDE. Gouvernance des données et interopérabilité dans le secteur public. Paris : OECD Publishing, 2022.
[27] CNIL. Biométrie : enjeux et cadre juridique de la protection des données. Paris : Commission nationale de l'informatique et des libertés, 2021.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

Conclusion

La gouvernance juridique des données sensibles dans le secteur public marocain apparaît aujourd'hui comme un enjeu central de la transformation numérique de l'État. L'administration contemporaine ne peut plus être pensée uniquement comme une structure de production de décisions, de prestations ou de services ; elle est également devenue une organisation productrice, détentrice, utilisatrice et responsable de données. Or, lorsque ces données concernent l'identité des personnes, leur santé, leur situation sociale, leurs droits, leurs parcours administratifs ou des infrastructures publiques critiques, leur traitement ne relève plus d'une simple gestion technique. Il engage directement la protection des droits fondamentaux, la confiance des citoyens, la continuité du service public, la sécurité juridique et la souveraineté numérique.

L'analyse menée permet de constater que le Maroc dispose déjà d'un socle juridique important pour encadrer ces enjeux. La loi n° 09-08 fournit les principes fondamentaux de protection des personnes à l'égard du traitement des données à caractère personnel. Elle permet d'organiser la licéité des traitements, l'information des personnes concernées, l'exercice de leurs droits, la sécurité des données, ainsi que l'encadrement des traitements sensibles et des transferts. La CNDP joue, dans cette architecture, un rôle essentiel de contrôle, d'autorisation, d'accompagnement et de régulation. À ce premier niveau s'ajoute la loi n° 05-20 relative à la cybersécurité, qui étend l'analyse au-delà de la donnée elle-même pour intégrer la protection des systèmes d'information, la résilience des infrastructures, la prévention des incidents et la continuité des services essentiels. L'encadrement du recours au cloud, enfin, marque une évolution importante en ce qu'il intègre les enjeux de dépendance technologique, de localisation, d'auditabilité, de réversibilité et de souveraineté opérationnelle.

Toutefois, l'existence de ces instruments juridiques ne suffit pas, à elle seule, à garantir une gouvernance effective. L'un des principaux résultats de cette étude est précisément de montrer que le défi majeur n'est pas seulement normatif, mais organisationnel. Le cadre juridique marocain n'est pas dépourvu de ressources ; il doit cependant être traduit en mécanismes concrets de pilotage, de contrôle et de preuve. La conformité ne peut plus être réduite à une déclaration, à une autorisation ou à une mention dans un cahier des charges. Elle doit être pensée comme un processus continu, fondé sur la cartographie des traitements, la classification des données, l'identification des responsables, l'encadrement des sous-traitants, la documentation des décisions, les analyses d'impact, les audits réguliers, la traçabilité des accès et la gestion structurée des incidents.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

La première partie de l'étude a permis de montrer que la qualification des données sensibles constitue le point de départ de toute gouvernance juridique. Cette qualification conditionne le niveau de protection applicable, les obligations procédurales, les mesures de sécurité, les restrictions d'accès, les règles de conservation et les mécanismes de contrôle. Dans le secteur public, cette qualification se complexifie en raison des finalités d'intérêt général, de l'interconnexion croissante des administrations, des obligations d'archivage, du droit d'accès à l'information et du recours à des prestataires externes. La gouvernance doit donc arbitrer entre plusieurs impératifs : protéger les personnes sans paralyser l'action administrative, permettre la circulation légitime de l'information sans créer de surveillance diffuse, assurer la transparence sans exposer les données sensibles, conserver les archives sans méconnaître les exigences de limitation et de proportionnalité.

La seconde partie a, quant à elle, mis en évidence la nécessité d'une gouvernance opérationnelle fondée sur la redevabilité. Face aux technologies émergentes, les risques ne sont plus seulement liés à la collecte ou à la conservation des données ; ils résultent aussi de la manière dont les données sont croisées, analysées, transférées, externalisées ou utilisées pour orienter des décisions publiques. L'intelligence artificielle introduit des risques d'opacité, de biais, de discrimination et de perte de contrôle humain. Le cloud soulève des questions de dépendance, de localisation, de maîtrise contractuelle et d'accès aux journaux d'audit. L'interopérabilité, l'IoT et la biométrie renforcent les risques de surveillance, de détournement de finalité et de diffusion incontrôlée des flux de données. Ces risques imposent une gouvernance fondée non seulement sur la conformité préalable, mais aussi sur la preuve continue de cette conformité.

Ainsi, l'hypothèse de départ se confirme : le droit marocain offre des fondations pertinentes pour construire une gouvernance juridique des données sensibles dans le secteur public, mais l'effectivité de cette gouvernance dépend de sa mise en œuvre institutionnelle et procédurale. Le véritable enjeu n'est donc pas de constater un vide juridique général, mais d'éviter une gouvernance fragmentée, dispersée entre protection des données, cybersécurité, cloud, commande publique, archivage et transparence administrative. La cohérence entre ces différents régimes devient la condition même de l'effectivité. Une administration peut être formellement conforme à une exigence isolée tout en demeurant structurellement vulnérable si elle ne dispose pas d'une vision intégrée des traitements, des risques, des responsabilités et des contrôles.

Dans cette perspective, plusieurs orientations peuvent être dégagées. Il apparaît nécessaire de renforcer la culture administrative de la donnée sensible, en imposant des démarches

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

systématiques de classification et de cartographie. Il convient également de consolider les mécanismes internes de gouvernance, par la mise en place de référents, de comités spécialisés, de procédures de validation des traitements à risque et de registres suffisamment documentés. La contractualisation avec les prestataires technologiques doit être pensée comme un instrument juridique de souveraineté et non comme une simple formalité technique : clauses d'audit, réversibilité, localisation, confidentialité, sécurité, notification des incidents, sous-traitance ultérieure et destruction des données doivent devenir des exigences centrales. Enfin, le recours à l'intelligence artificielle, à la biométrie, à l'IoT ou aux systèmes interconnectés doit être précédé d'analyses d'impact et accompagné de mécanismes de supervision humaine, d'explicabilité, de traçabilité et de contrôle ex post.

En définitive, la gouvernance juridique des données sensibles dans le secteur public marocain doit être comprise comme une méthode de transformation du droit en pratiques administratives vérifiables. Elle permet de dépasser l'opposition artificielle entre innovation technologique et protection des droits. L'enjeu n'est pas de freiner la modernisation numérique de l'administration, mais de l'encadrer juridiquement afin qu'elle demeure compatible avec les exigences de l'État de droit, de la sécurité, de la transparence et de la confiance publique. Dans un environnement marqué par l'intelligence artificielle, le cloud, l'interconnexion et la circulation massive des données, la donnée sensible ne peut être gouvernée efficacement que par une approche intégrée, préventive et probatoire. C'est à cette condition que le secteur public marocain pourra concilier efficacité administrative, souveraineté numérique et protection effective des droits fondamentaux.

L'apport principal de cette recherche est de proposer une lecture intégrée de la gouvernance juridique des données sensibles dans le secteur public marocain. En articulant la protection des données personnelles, la cybersécurité, l'encadrement du cloud, les usages de l'intelligence artificielle et l'exigence de redevabilité administrative, l'étude dépasse une approche fragmentée de la conformité juridique. Elle met en évidence que la protection effective des données sensibles ne dépend pas uniquement de l'existence de textes normatifs, mais aussi de la capacité des administrations publiques à organiser des mécanismes concrets de gouvernance, de contrôle, d'audit, de traçabilité et de responsabilisation. Ainsi, la contribution de cette recherche réside dans la construction d'une grille de lecture opérationnelle permettant de concilier innovation technologique, sécurité juridique, souveraineté numérique et protection des droits fondamentaux des citoyens.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

BIBLIOGRAPHIE

I. Ouvrages et articles doctrinaux

Bensamoun, A., & Loiseau, G. (2021). *Droit du numérique : contrats, innovation, données et gouvernance*. Paris : Eyrolles.

Bellan, C. (2022). *La gouvernance algorithmique et la transformation de l'action publique*. Paris : L'Harmattan.

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford : Oxford University Press.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1-33.

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (dir.). (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford : Oxford University Press.

Lessig, L. (2006). *Code: Version 2.0*. New York : Basic Books.

Millard, C. (dir.). (2013). *Cloud Computing Law*. Oxford : Oxford University Press.

Moalla, N., Ouzrout, Y., & Bouras, A. (2018). *Interopérabilité des systèmes d'information d'entreprise : concepts et architectures*. Paris : Hermès Science Lavoisier.

Price, W. N. (2018). Black-box medicine. *Harvard Journal of Law & Technology*, 28(2), 419-467.

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 59-68.

Van Alsenoy, B. (2019). *Data Protection Law in the EU: Roles, Responsibilities and Liability*. Cambridge : Intersentia.

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, 31(2), 841-887.

Zerilli, J., Knott, A., Maclaurin, J., & Gavaghan, C. (2019). Transparency in algorithmic and human decision-making: Is there a double standard? *Philosophy & Technology*, 32(4), 661-683.

II. Rapports, guides et références institutionnelles

Agence Nationale de la Sécurité des Systèmes d'Information. (2019). *SecNumCloud : référentiel de sécurité pour les services cloud*. Paris : ANSSI.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. (2020). *Délibération n° D-188-2020 du 14 décembre 2020 relative à l'analyse d'impact sur la protection des données*. Rabat : CNDP.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. (2021). *Guide pratique sur la conformité à la protection des données personnelles au Maroc*. Rabat : CNDP.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. (2023). *Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel : texte consolidé*. Rabat : CNDP.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. (2023). *Rapport annuel d'activité*. Rabat : CNDP.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. (2025). *IA et protection des données à caractère personnel*. Rabat : CNDP.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. (2025). *Délibération n° D-943-2025 du 28 novembre 2025 relative au modèle type de demande d'autorisation pour le traitement des données à caractère personnel recueillies dans le cadre du contrôle d'accès à des lieux professionnels privés*. Rabat : CNDP.

Commission Nationale de l'Informatique et des Libertés. (2024). *Guide de la sécurité des données personnelles*. Paris : CNIL.

Commission Nationale de l'Informatique et des Libertés. (2025). *Développement des systèmes d'intelligence artificielle : recommandations pour respecter le RGPD*. Paris : CNIL.

Direction Générale de la Sécurité des Systèmes d'Information. (2020). *Note de présentation de la loi n° 05-20 relative à la cybersécurité*. Rabat : DGSSI.

Direction Générale de la Sécurité des Systèmes d'Information. (2024). *Références et textes relatifs à la cybersécurité*. Rabat : DGSSI.

European Data Protection Board. (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. Brussels : EDPB.

European Union Agency for Cybersecurity. (2021). *Cloud Security for Healthcare Services*. Athens : ENISA.

European Union Agency for Cybersecurity. (2021). *Cloud Security: Recommendations and Good Practices*. Athens : ENISA.

Ministère de la Transition Numérique et de la Réforme de l'Administration. (2024). *Digital Morocco 2030 : stratégie nationale de transformation numérique*. Rabat.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Washington, D.C. : U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1*. Washington, D.C. : U.S. Department of Commerce.

Organisation de Coopération et de Développement Économiques. (2019, mise à jour 2024). *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449*. Paris : OCDE.

Organisation de Coopération et de Développement Économiques. (2022). *Gouvernance des données et interopérabilité dans le secteur public*. Paris : OECD Publishing.

III. Normes, standards et référentiels techniques

International Organization for Standardization. (2013). *ISO/IEC 27001: Information Security Management Systems — Requirements*. Genève : ISO.

International Organization for Standardization. (2014). *ISO/IEC 27017: Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*. Genève : ISO.

International Organization for Standardization. (2019). *ISO/IEC 27018: Code of Practice for Protection of Personally Identifiable Information in Public Clouds Acting as PII Processors*. Genève : ISO.

International Organization for Standardization. (2022). *ISO/IEC 27002: Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. Genève : ISO.

International Organization for Standardization. (2023). *ISO/IEC 42001: Artificial Intelligence Management System*. Genève : ISO.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework 2.0*. Washington, D.C. : U.S. Department of Commerce.

IV. Textes juridiques et réglementaires marocains

Constitution du Royaume du Maroc du 1er juillet 2011, notamment les articles 24 et 27 relatifs à la protection de la vie privée et au droit d'accès à l'information.

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.

Décret n° 2-09-165 du 25 joumada I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 36 Juin 2026

Loi n° 31-13 relative au droit d'accès à l'information, promulguée par le dahir n° 1-18-15 du 5 joumada II 1439 (22 février 2018).

Loi n° 69-99 relative aux archives, promulguée par le dahir n° 1-07-167 du 19 kaada 1428 (30 novembre 2007).

Loi n° 05-20 relative à la cybersécurité, promulguée par le dahir n° 1-20-69 du 4 hija 1441.

Décret n° 2-24-921 du 18 rabii II 1446 (22 octobre 2024) relatif au recours aux prestataires de services cloud par les entités et les infrastructures d'importance vitale disposant de systèmes d'information sensibles.

V. Instruments internationaux et textes comparés

Conseil de l'Europe. (1981). *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Convention 108. Strasbourg.

Conseil de l'Europe. (2018). *Protocole d'amendement à la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Convention 108+. Strasbourg.

Conseil de l'Europe. (2024). *Convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit*. Strasbourg.

Union africaine. (2014). *Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel*, dite Convention de Malabo. Malabo.

Union européenne. (2016). *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, Règlement général sur la protection des données.

Union européenne. (2022). *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données*, Data Governance Act.

Union européenne. (2022). *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union*, Directive NIS 2.

Union européenne. (2023). *Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'accès équitable aux données et leur utilisation*, Data Act.

Union européenne. (2024). *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle*, Artificial Intelligence Act.