INTERNATIONAL JOURNAL OF RESEARCH IN ECONOMICS AND FINANCE, 2025, Vol. 2, No. 8, 75-84. https://doi.org/10.71420/ijref.v2i8.141

La souveraineté numérique : Une analyse juridico- technique, cas du Maroc
Digital sovereignty: A legal-technical analysis, the case of Morocco

Farouk GHARBAOUI
Laboratoire de Gouvernance publique, politiques publiques et études administratives internationales et douanières, Faculté des Sciences Juridiques, Économiques et Sociales de Ain Chock, Université Hassan 2, Casablanca, Maroc.

Résumé. Cette étude juridico-technique analyse l'infrastructure web nationale marocaine sous l'angle de la souveraineté numérique et du droit à porter extraterritorial. À travers l'analyse approfondie de 414 sites web institutionnels marocains, nous mettons en évidence les implications juridiques des choix d'infrastructure technique. Les résultats révèlent des faiblesses significatives : 64% des sites analysés n'utilisent pas de protocole SSL, 81% n'ont pas de politique de confidentialité, et 40% des sites sont hébergés hors du territoire national. Ces constats soulèvent des questions cruciales sur la protection des données personnelles et la souveraineté numérique du Maroc mais plus que comment on est arrivé à cette situation il faut étudier son étiologie et présenter les quelques conséquences qui en découlent.

Mots-clés : Souveraineté numérique ; Infrastructure web ; Droit international ; Protection des données ; Maroc.

Abstract. This legal and technical study analyzes Morocco's national web infrastructure through the lens of digital sovereignty and extraterritorial legal exposure. By conducting an in-depth review of 414 institutional Moroccan websites, we highlight the legal implications of technical infrastructure choices. The findings reveal significant vulnerabilities: 64% of the websites analyzed do not use SSL protocols, 81% lack a privacy policy, and 40% are hosted outside the national territory. These observations raise critical concerns regarding personal data protection and Morocco's digital sovereignty. Beyond understanding how such a situation emerged, it is essential to examine its etiology and to outline the resulting consequences.

Keywords : *Digital Sovereignty, Web Infrastructure, International Law, Data Protection, Morocco.*

1. Introduction

La généralisation des infrastructures numériques modifie profondément l'exercice classique de la souveraineté : la localisation technique d'un serveur, la couche logicielle qui l'exploite ou le contrat d'hébergement qui l'encadre deviennent autant de variables géopolitiques que juridiques (Kuner, 2020). Les États ne contrôlent plus seulement des frontières physiques ; ils négocient, contestent ou délèguent la maîtrise de flux de données qui empruntent des nuages informatiques transnationaux et s'inscrivent, de facto, sous plusieurs ordres normatifs à la fois. Dans l'espace euro-méditerranéen, l'Union européenne a donné la mesure de cette extraterritorialité normative en étendant le RGPD aux organisations établies hors de son territoire mais traitant les données de ses résidents (Van Alsenoy, 2019). De son côté, le Congrès américain a renforcé par le CLOUD Act la possibilité pour les autorités fédérales d'accéder aux contenus détenus par des fournisseurs relevant de la juridiction des États-Unis, quel que soit l'emplacement physique des serveurs. Ces instruments illustrent la tension entre une souveraineté qui reste, en théorie, territoriale et une architecture du réseau qui, elle, demeure globalisée (Cohen, 2019).

Dans ce contexte, le Maroc, récemment présenté comme le premier hub africain en nombre de data-centres actifs[1], se trouve à la croisée de deux impératifs : capitaliser sur la connectivité internationale pour stimuler l'investissement et, simultanément, préserver l'intégrité de son ordre public numérique. Les lignes stratégiques énoncées dans « Maroc Digital 2030 » appellent d'ailleurs à renforcer l'autonomie technologique du pays, mais la littérature scientifique reste lacunaire sur l'articulation concrète entre droit interne, traités multilatéraux et choix d'infrastructure.

À partir de ce constat, cette recherche s'articule autour de trois questions principales : (1) dans quelle mesure l'infrastructure web des institutions marocaines reflète-t-elle ou fragilise-t-elle la souveraineté numérique du Royaume ? (2) quelles vulnérabilités juridiques et techniques résultent de l'hébergement hors territoire national et du déficit de conformité aux normes de protection des données ? (3) enfin, quels leviers réglementaires et institutionnels permettraient d'assurer une souveraineté numérique effective et opérationnelle ?

Pour y répondre, l'étude s'appuie sur un corpus de 414 sites institutionnels marocains, couvrant administrations, agences publiques et établissements académiques. Ce choix permet de dépasser l'analyse de cas isolés pour restituer une image d'ensemble de l'écosystème numérique national et de ses fragilités.

C'est en croisant cette cartographie inédite avec une analyse juridique multiscalaire que ce travail entend combler ce vide. En articulant données techniques et cadres normatifs, il propose une lecture intégrée des enjeux de souveraineté numérique, rarement abordée de manière empirique et comparative dans le contexte marocain.

L'étude proposée inscrit donc la souveraineté numérique marocaine dans une triple perspective: descriptive, en dressant la cartographie de 414 sites institutionnels ; analytique, en confrontant les pratiques observées aux exigences juridiques ; critique, enfin, en évaluant la cohérence des politiques publiques avec les ambitions affichées. Sur le plan méthodologique, nous croisons une approche d'ingénierie inverse – crawler Python pour la collecte d'adresses IP et géolocalisation des serveurs – avec une grille d'analyse normative qui mobilise la loi 09-08, le RGPD, le Stored Communications Act de 1986 et son amendement par le CLOUD Act de 2018.

Le reste de l'article est structuré comme suit : la première section présente en détail la méthodologie déployée ; la deuxième expose les résultats empiriques issus de l'analyse ; la troisième discute les implications juridiques et institutionnelles ; enfin, la conclusion revient sur les enseignements majeurs et propose des pistes pour renforcer la souveraineté numérique du Maroc.

2. Méthodologie

Le corpus de 414 sites web a été constitué par un processus de cartographie systématique : à partir d'un site pivot (mjcc.ma), un robot crawler développé en Python a recensé les interconnexions hypertextes permettant d'identifier d'autres sites institutionnels liés. Ce mode de constitution garantit que les sites étudiés appartiennent bien à l'écosystème institutionnel marocain et qu'ils entretiennent entre eux une cohérence fonctionnelle. L'approche ainsi retenue vise à assurer à la fois l'exhaustivité et la représentativité du corpus, tout en permettant une exploitation comparative des résultats (Figure 1)[2]. Nous avons également mis en place un système de géolocalisation des serveurs en exploitant des bases de données publiques. Cette

[1] Voir : https://algeriatimes.info/article/morocco-overtakes-south-africa-as-africas-top-data-center-hub?utm_source=chatgpt.com

[2] Le logiciel qui a été utilisé a été développé par l'auteur de cet article qui est accessible sur la base de données du site web Github qui héberge les codes utilisés pour le développement de site, logiciel et application.

méthodologie repose sur la collecte des adresses IP des sites analysés et leur envoi à des services de géolocalisation[3] qui identifient la localisation physique des serveurs correspondants (**Figure 2**). Par ailleurs, des outils de reconnaissance de texte ont été employés pour examiner les politiques de confidentialité disponibles, en identifiant leur présence, leur contenu, et leur accessibilité et déterminer si les sites visités sont conformes aux dispositions des lois en vigueur comme la loi 09.08 ou dans certaines situation au RGPD en respectant le principe du ciblage[4]. Par cette méthode nous avons essayé d'analyser la conformité aux exigences de la loi 09.08 mais aussi au RGPD si ça s'applique des sites web Marocain principalement gouvernementaux, institutionnels, académiques, médias et autres. L'intérêt est de déterminer selon la situation de l'infrastructure et le contenu des sites web quelles dispositions des lois et des conventions s'y appliquent. Un site hébergé sur un serveur se trouvant aux Etats unis est sous le cadre légale des dispositions des lois américaines principalement le *Stored Communications Act et plus récemment le Clarifying Lawful Overseas Use of Data Act* connu sous le nom de Cloud Act qui permet aux autorités américaines d'exiger la remise de contenus stockés sur un serveur étranger d'une entité local[5]. Un site web qui cible des utilisateurs se trouvant en Europe se voit régit par le RGPD. Une configuration particulière fera l'objet de notre étude est celle d'avoir un site web hébergé au Maroc auprès d'un hébergeur Marocain et pourtant tombe sous les dispositions des lois étrangères qu'on va analyser plus en détail.

3. Résultats

Les résultats qui suivent permettent d'apporter des éléments de réponse aux trois questions de recherche posées en introduction, en mettant en lumière l'état de l'infrastructure web institutionnelle marocaine, ses vulnérabilités et ses implications juridiques.

a. Etat des lieux

Notre analyse des sites web nous a permis de déterminer que partant d'un point central en l'occurence le site mjcc.ma d'analyser 414 sites web tous relié entre eux (Figure 1), l'intérêt était de relever que les sites web analysé étaient véritablement existant preuve est leur référence indiqué sur les autres sites web. Les résultats préliminaires (Figure 3) montre que même si certains sites web sont présenter et leur lien existe ils ne sont pas accessible, pour ce qui est de la localisation physique des serveurs qui stock principalement les fichiers du sites web ce qu'on appelle un serveur web (Figure 2) seuls 250 sites des 414 sont hébergés au Maroc, tandis que 164 sites ont une infrastructures située à l'étranger, avec une concentration notable en Amérique du Nord (114 sites). L'analyse nous a permis aussi de déterminer la situation de la conformité des sites web à l'égard des dispositions de la loi 09.08, à peine 19% des sites web analyser avait une indication sur les mesures prises à l'égard du traitement des données à caractère personnel et sur ces 19% seuls 40% avait fait une déclaration au préalable au CNDP et ont obtenu un numéro d'agrément. Depuis le dernier rapport du CNDP paru en 2016 qui indiquait que seul 8% des sites web sur un total de 167 analyser était conforme6 on s'aperçoit qu'après presque

[3] DNSChecker est un site qui permet la géolocalisation et la présentation d'informations qui sont réputées accessibles selon les normes internationales de télécommunications. voir : https://dnschecker.org

[4] Article 3 paragraphe 2 du RGPD

[5] Nouvel article § 2713 du Stored Communications Act (inséré par § 103(a)) :
« …shall comply with the obligations of this chapter to preserve, backup, or disclose … regardless of whether such communication … is located within or outside of the United States. ». a donc introduit l'extraterritorialité : dès qu'un tribunal américain délivre un subpoena, un mandat 18 U.S.C. § 2703 ou un ordre de perquisition, le fournisseur doit obéir même si les fichiers se trouvent sur un data-center européen, asiatique ou africain mais sinon avant le Cloud act tout contenu stocker sur un serveur se trouvant sur le territoire américain était accessible par les autorités moyennant mandat.

[6] CNDP, *Rapport d'activité 2016* (Controle des sites web) p. 51

une décennie la situation ne s'est pas beaucoup améliorée. Au-delà du constat sur la situation de l'infrastructure et de la conformité, l'analyse nous a amené à déterminer les facteurs qui ont abouti à cette situation qui d'ailleurs soulève des questions juridiques majeures, notamment la portée des lois des pays étrangers sur ces sites web institutionnels marocains.

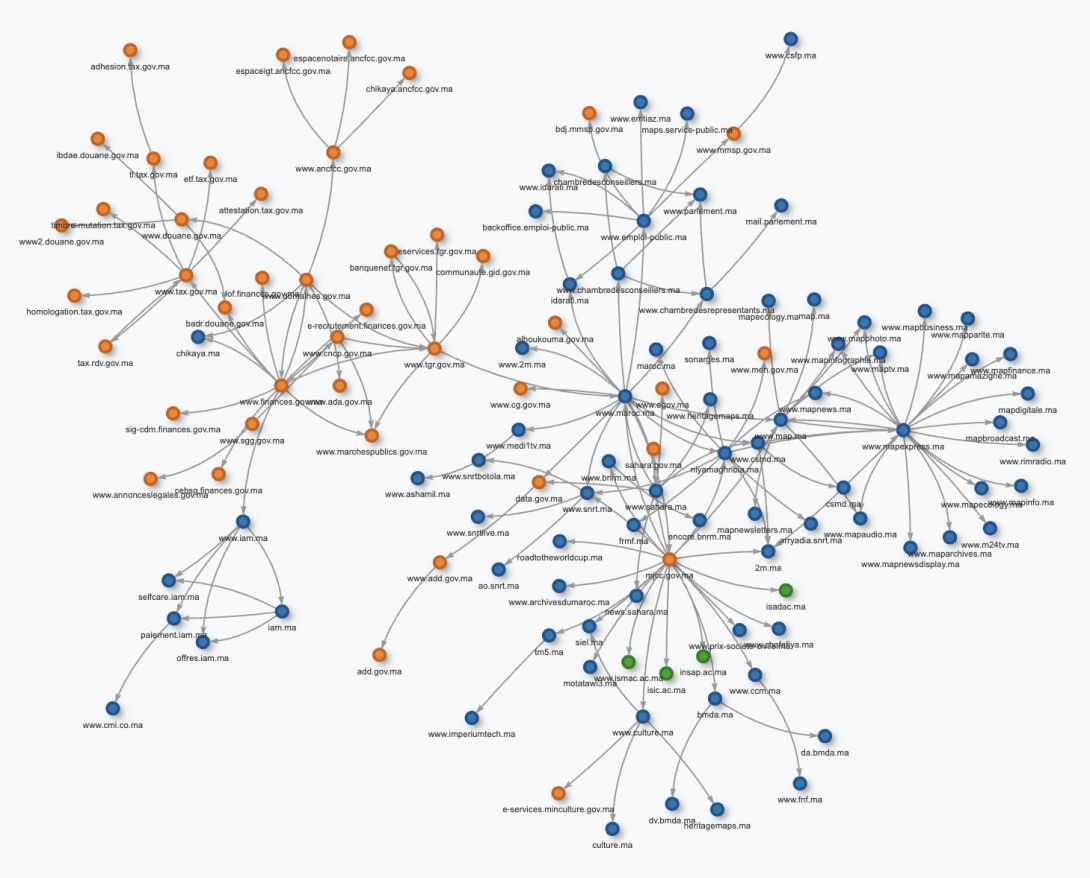

Figure 1 : Le graphique illustre un extrait des sites web visité et analyse

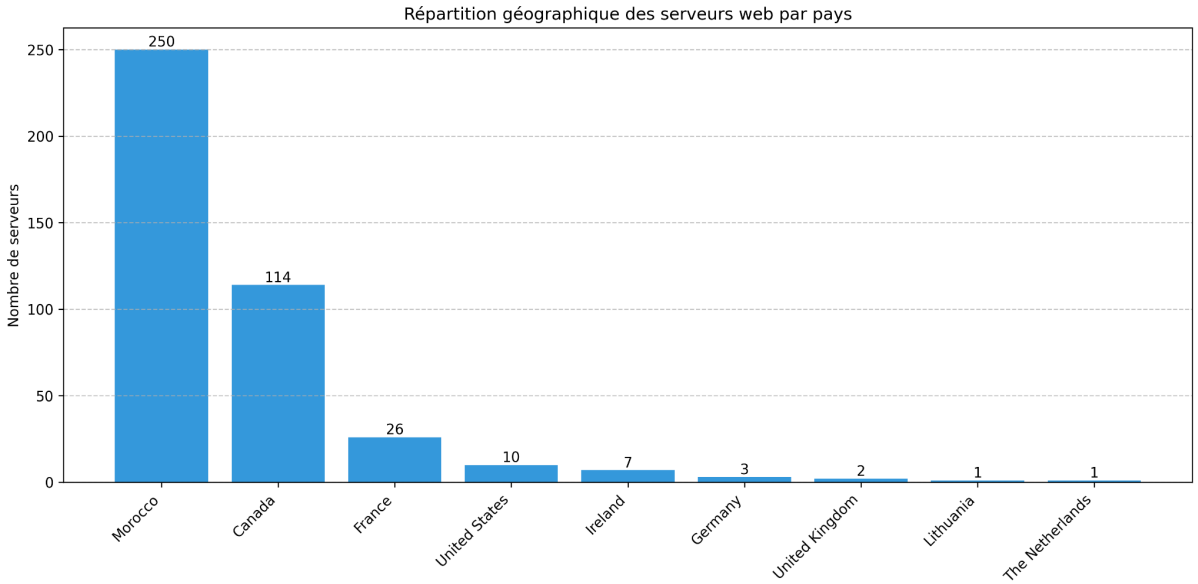

Figure 2 : Répartition géographique des serveurs web par pays des sites web Marocains

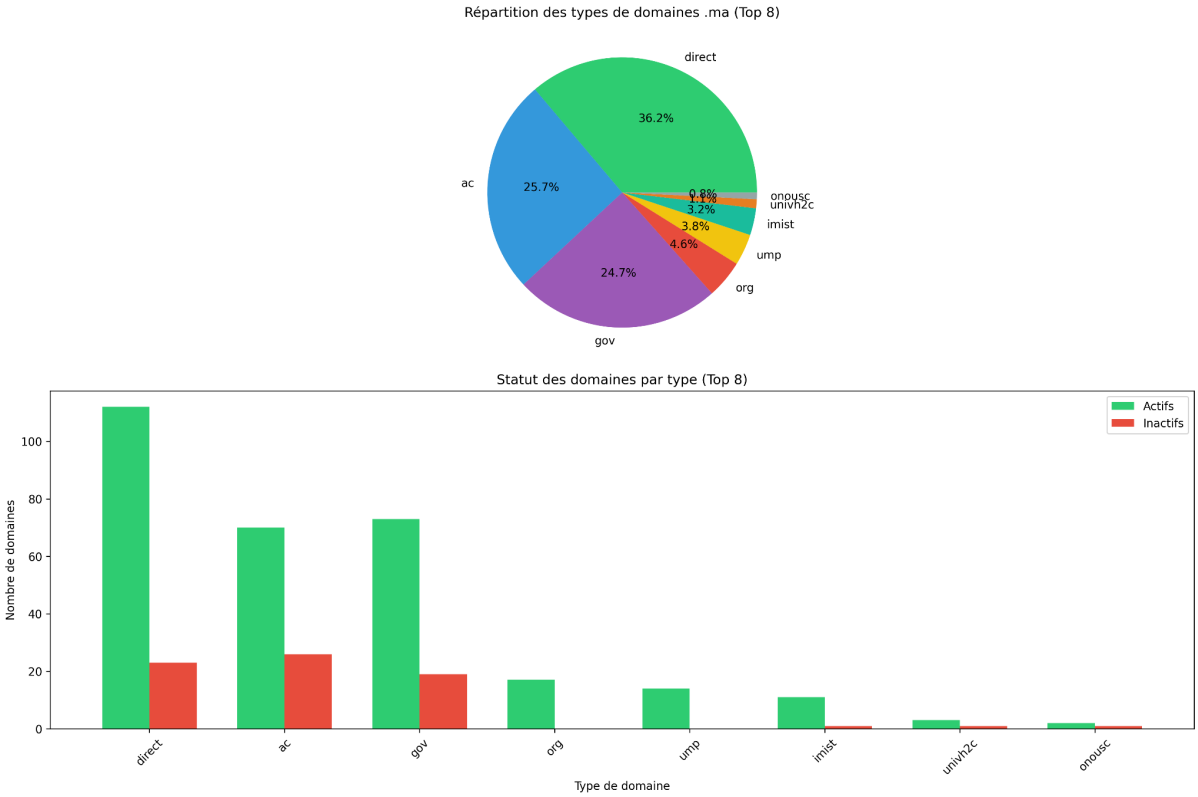

Figure 3 : Répartition des types de domaines analyser et leur statuts (actifs ou inactifs)

b. Origines structurelles et hypothèses explicatives

Ce panorama chiffré met en lumière une situation préoccupante, tant du point de vue de la localisation technique des infrastructures que du respect des cadres légaux en vigueur. Mais au-delà de ces constats empiriques, il convient désormais d'en interroger les causes profondes et les dynamiques systémiques. Comprendre les logiques institutionnelles, réglementaires et techniques qui ont conduit à cette configuration permet d'ouvrir une réflexion plus large sur les mécanismes d'implémentation ou d'évitement de la souveraineté numérique.

C'est dans cette perspective que l'analyse mobilise deux études de cas contrastées mais représentatives de l'écosystème institutionnel marocain, afin d'illustrer les décalages entre les intentions souverainistes et les réalités opérationnelles.

c. Études de cas : entre ambition souverainiste et contraintes structurelles

Afin d'objectiver la discussion normative, l'article mobilise deux études de cas contrastées mais représentatives de l'écosystème institutionnel marocain : d'une part, le nouveau portail de l'Agence urbaine de Berrechid-Benslimane, fruit du marché n° 02/2025/AUBB, dont le cahier des prescriptions spéciales impose un hébergement « exclusivement … sur des serveurs en mode cloud localisés au Maroc » et assortit cette exigence d'un niveau Tier 3 et d'un dispositif de supervision 24/7/365 ; d'autre part, la commande public de la Wilaya Tanger-Tétouan-Al Hoceïma (Tableau 1) pour la création et l'hébergement d'un site web sans clause de localisation ni protocole de réplication sur le territoire national. Le premier cas fournit le scénario maximaliste d'un « hébergement souverain » voulu par une entité publique locale : il permet de tester l'articulation entre les prescriptions du marché public, la loi 09-08 et les obligations de

conservation prévues par le décret n° 2-22-431 sur les marchés publics. Le second, au contraire, soulève la question de la soumission concurrente au RGPD dès lors que des utilisateurs européens consultent le portail et au CLOUD Act, si le fournisseur opte un hébergement sur Amazon Web Service us-east-1 relèvent de la juridiction fédérale américaine. L'analyse croisée de ces configurations, l'une ancrée dans un datacenter casablancais, l'autre déterritorialisée dans un cloud transatlantique, sert de fil conducteur pour évaluer la portée effective des normes nationales de souveraineté numérique et la capacité des maîtres d'ouvrage à concilier ouverture internationale, conformité réglementaire et maîtrise opérationnelle des données.

Le cahier des prescriptions spéciales n° 02/2025 de l'Agence urbaine de Berrechid-Benslimane retient, pour l'hébergement de son Système d'information géographique et de son site institutionnel, une clause apparemment maximaliste : « serveurs en mode cloud hébergés et localisés au Maroc, grade Tier 3 ». À première vue, cette exigence installe le marché public dans une position de souveraineté numérique forte ; elle réduit le risque de transfert incontrôlé de données, satisfait à l'article 43 de la loi 09-08 sur la protection des données personnelles et répond, de surcroît, aux recommandations de la CNDP visant à « favoriser prioritairement l'hébergement national » (CNDP, 2024). Pourtant la localisation matérielle n'est qu'une variable parmi d'autres dans l'équation juridique. L'agence recourt, selon le même CPS, à un « mode cloud » ; or la quasi-totalité des opérateurs certifiés Tier 3 au Maroc fonctionne sous licence logicielle ou sous structure capitalistique relevant d'éditeurs états-uniens ou européens. Pour mieux comprendre regardons de plus prêt qu'est ce qu'implique le Tier 3, Un « Tier 3 » garantit uniquement le *niveau de disponibilité* de la salle informatique (redondance N+1, maintenance sans arrêt, 72 h d'autonomie-énergie, etc.) selon la méthodologie de l'Uptime Institute : l'infrastructure est « concurrently maintainable », pas forcément « hébergée chez un opérateur national »[7].

En pratique, pour atteindre cette cible, la quasi-totalité des data-centres marocains s'appuient sur des briques logicielles propriétaires importées : hyperviseurs (VMware vSphere, Microsoft Hyper-V, Oracle KVM), outils d'orchestration (vCenter/vCloud, System Center, Cisco UCS-M), plateformes de sauvegarde ou de stockage (Dell EMC, NetApp ONTAP, Veeam). Ces produits sont fournis sous contrat de licence que les éditeur souvent américains imposent en droit californien ou fédéral, avec clauses d'export-control et de conformité aux lois US. On lit par exemple dans les *Cisco End-User License Terms* : « This Agreement is governed by the laws of the State of California… »[8], et, dans l'EULA générique VMware, l'utilisateur accepte la loi et la juridiction de Santa Clara County (Cal.).

Dès lors que le prestataire offrant les services d'hébergement Tier 3 est affilié à AWS, Microsoft ou Google, le Stored Communications Act, tel que modifié par le CLOUD Act, permet toujours à une autorité fédérale américaine d'exiger la remise de contenus détenus « dans la possession ou sous le contrôle » d'un fournisseur soumis à sa juridiction, quel que soit l'endroit où les octets reposent physiquement (US Congress, 2018). Le bouclier territorial se trouve ainsi relativisé : l'agence demeure exportatrice potentielle de données par l'intermédiaire de son sous-traitant, et elle reste responsable in solidum devant l'usager marocain en cas d'atteinte à la confidentialité.

Le second angle d'analyse concerne l'extraterritorialité du RGPD. Le portail de l'AUBB, bien que orienté vers des démarches foncières locales, propose des fonctionnalités de consultation

[7] Economizers in Tier Certified Data Centers, Voir : https://journal.uptimeinstitute.com/implications-of-economizers-in-tier-certified-data-centers/

[8] Paragraphe 12.8 du "Cisco End User License Agreement" indique que tout produit Ciso est assujetie au control d'export et sanction légale des États Unies.

cartographique susceptibles d'être utilisées par des investisseurs européens ; le simple fait de « cibler » ces utilisateurs, au sens de l'article 3 § 2 du règlement, déclenche l'application du RGPD, lequel impose une base légale de traitement, une information renforcée et, en cas de transfert ultérieur, la mise en place de clauses contractuelles types ou de mesures techniques additionnelles (EDPB, 2021). À défaut de représentant dans l'UE ou de registre de traitement mis à jour, l'agence s'expose à un cumul d'obligations contradictoires : d'un côté la CNDP lui demande de maintenir les données sur le territoire, de l'autre l'Union européenne lui impose des garanties équivalentes à celles de l'EEE pour tout accès par un fournisseur non européen.

Dans ce faisceau d'injonctions, la solution durable ne réside ni dans la seule relocalisation, ni dans une dépendance aveugle aux opérateurs globaux, mais dans la combinaison de trois leviers. D'abord, un chiffrement de bout en bout dont la clé maîtresse reste détenue par une autorité publique marocaine, condition sine qua non pour neutraliser les effets d'une requête extraterritoriale la jurisprudence récente aux États-Unis montre que les autorités renoncent lorsque la donnée est chiffrée et que la clé n'est pas accessible au fournisseur (Swire & Hem, 2020). Ensuite, la contractualisation détaillée de la chaîne de sous-traitance, incluant l'obligation pour le prestataire cloud de notifier toute demande légale étrangère et de contester les réquisitions non conformes à la « comity analysis » du § 2703 (h) SCA. Enfin, la réalisation d'une analyse d'impact relative à la protection des données dès la phase de conception du SIG, afin d'identifier les traitements visant des usagers européens et de prévoir, le cas échéant, un représentant dans l'UE comme l'autorise l'article 27 du RGPD.

Ainsi, loin d'être un simple détail technique, la mention « serveurs localisés au Maroc » ouvre un champ de tensions entre droit interne, droit conventionnel et droits étrangers. Seule une approche intégrée localisation raisonnée, gouvernance contractuelle et sécurisation cryptographique – peut convertir la clause souverainiste du CPS en protection juridique effective. À cette condition, la promesse d'un « mode cloud » national devient crédible et l'Agence urbaine peut concilier ouverture de ses données cartographiques et préservation de la souveraineté informationnelle du Royaume.

4. Conclusion

Au terme de cette étude, il apparaît que la souveraineté numérique ne peut se résumer à une simple volonté politique ou à des mesures techniques ponctuelles, mais qu'elle suppose la mise en place d'une architecture juridique et institutionnelle cohérente, capable de répondre aux défis de l'interdépendance technologique globale. La cartographie des sites institutionnels marocains a révélé l'ampleur de la fragmentation actuelle, tant en matière d'hébergement que de conformité aux normes de protection des données. Les tensions identifiées entre droit interne, obligations extraterritoriales et choix technologiques illustrent le besoin d'une structuration systémique et intégrée de la souveraineté numérique.

D'un point de vue normatif, il est indispensable que le Maroc élargisse l'approche de la loi 09-08 à des concepts contemporains tels que la responsabilité active du responsable de traitement (accountability), la protection des données dès la conception "privacy by design" (A.Cavoukian, 2009)[9], ou encore les analyses d'impact (DPIA) comme instruments anticipatoires. Ces principes, aujourd'hui ancrés dans les standards européens, notamment le RGPD, et repris dans les recommandations du Comité européen de la protection des données (EDPB)[10], devraient être transposés dans une future réforme de la législation nationale ou à tout

[9] CAVOUKIAN, Ann, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2009.

[10] Comité européen de la protection des données (EDPB), *Recommandations 01/2020 sur les mesures à prendre pour garantir la conformité des transferts de données personnelles*, version révisée du 18 juin 2021.

le moins dans une charte d'hébergement souverain applicable aux administrations publiques.

Sur le plan institutionnel, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) joue déjà un rôle central dans la définition et la mise en œuvre de la politique nationale de cybersécurité. Elle assure notamment la veille, l'alerte et la gestion des incidents via le maCERT, édicte des référentiels techniques en matière de sécurité des systèmes d'information, mène des audits auprès des administrations publiques et coordonne les efforts de formation et de sensibilisation dans les secteurs sensibles.

Cependant, dans un contexte de numérisation croissante des services publics et de dépendance accrue aux infrastructures numériques, il demeure essentiel de consolider ce rôle en lui adjoignant un pôle technique autonome et renforcé, à même d'élargir son action vers la supervision systématique des marchés publics liés au numérique, la certification des prestataires nationaux, et la vérification de la conformité effective des solutions déployées aux standards nationaux en matière de sécurité, de localisation des données et de résilience.

Une telle évolution contribuerait à rendre plus opérationnelle et intégrée l'architecture institutionnelle marocaine de cybersécurité, en inscrivant la sécurité numérique au cœur même des procédures de commande publique et de déploiement des infrastructures critiques. Elle permettrait également d'assurer une meilleure articulation entre protection des données personnelles et sécurité des systèmes d'information, deux volets indissociables de toute politique cohérente de souveraineté numérique.

Mais une souveraineté numérique pérenne ne pourra émerger sans une transformation culturelle profonde des pratiques de l'administration. La formation des décideurs publics aux enjeux juridiques et stratégiques du numérique doit devenir une priorité. Une montée en compétence et l'introduction d'une obligation de formation en protection des données, en cybersécurité et en gestion des dépendances technologiques dans le cursus des hauts cadres publics et dans les marchés informatiques constituerait une avancée significative. Il en va non seulement de la conformité des systèmes, mais également de la capacité de l'État à défendre ses intérêts stratégiques dans un contexte international marqué par la montée du cloud geopolitics[11].

Enfin, l'autonomisation technique doit s'accompagner de mécanismes concrets de résilience : chiffrement de bout en bout avec gestion souveraine des clés, contractualisation exigeante de la chaîne de sous-traitance, clauses de notification obligatoire en cas de requête juridique étrangère, et présence institutionnelle dans l'Union européenne pour assurer la conformité au RGPD lors du traitement de données de ressortissants européens. Ces leviers ne sont pas théoriques : ils constituent les seuls remparts effectifs face à l'extraterritorialité normative grandissante des puissances numériques dominantes (Swire, P. & DeBrae Kennedy-Mayo, 2021)[12].

La souveraineté numérique ne saurait donc se penser comme un retranchement mais comme une stratégie d'équilibre entre ouverture, sécurité juridique et maîtrise opérationnelle. À cette condition, le Maroc pourra asseoir une posture de confiance numérique alignée sur ses objectifs de développement, d'attractivité économique et de respect des droits fondamentaux dans le cyberespace.

[11] De Filippi, P. & Hassan, S. (2016), « Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code », *First Monday*, vol. 21, n°12 ; Cohen, J. E. (2019), *Between Truth and Power. The Legal Constructions of Informational Capitalism*, Oxford University Press.

[12] En avril 2021, la CNPD portugaise (Comissão Nacional de Proteção de Dados) a ordonné à l'Institut national de la statistique (INE) de suspendre le transfert de données personnelles vers les États-Unis, car celles-ci étaient traitées dans le cadre d'un contrat avec la société Cloudflare, un fournisseur américain.

5. Bibliographie

- Règlement général sur la protection des données (RGPD), article 3, paragraphe 2. *(Portée extraterritoriale du RGPD en cas de traitement de données visant des personnes dans l'UE, même par des entités non établies dans l'Union.)*
- Stored Communications Act, § 2713 (modifié par le CLOUD Act, § 103(a)), 18 U.S.C. § 2703.
  « …shall comply with the obligations of this chapter to preserve, backup, or disclose … regardless of whether such communication … is located within or outside of the United States. »
- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP), *Rapport d'activité 2016*, Rabat, p. 51. *(Contrôle des sites web institutionnels et conformité avec la loi 09-08.)*
- Uptime Institute, *Implications of Economizers in Tier Certified Data Centers*, consulté en ligne : https://journal.uptimeinstitute.com/implications-of-economizers-in-tier-certified-data-centers
  Cisco Systems, *End User License Agreement*, paragraphe 12.8. *(Soumission des produits Cisco aux réglementations d'exportation américaines et aux sanctions du Department of Commerce.)*
- Cavoukian, Ann, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2009. *(Document fondateur sur l'intégration de la vie privée dans la conception des systèmes numériques.)*
- Comité européen de la protection des données (EDPB), *Recommandations 01/2020 sur les mesures à prendre pour garantir la conformité des transferts de données personnelles*, version révisée du 18 juin 2021.
- De Filippi, Primavera & Hassan, Samer, « Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code », *First Monday*, vol. 21, n° 12, 2016.
- Cohen, Julie E., *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019.
- Comissão Nacional de Proteção de Dados (CNPD – Portugal), *Décision d'avril 2021* ordonnant à l'Institut national de la statistique (INE) de suspendre le transfert de données vers les États-Unis dans le cadre d'un contrat avec Cloudflare. *(Illustration du rejet européen des transferts non conformes post-Schrems II.)*

Annexe :

Tableau 1 : Appels d'offres publics (2025) – niveau de souveraineté exigé pour l'hébergement des sites et plateformes

Avis / séance d'ouverture	AO n° & intitulé abrégé	Maître d'ouvrage (MO)	Prestations principales	Exigence d'hébergement souverain ?	Formulation / observation
24/03/2025	047-25 — Maintenance du site web	Office National des Aéroports (ONDA)	MCO + infogérance	Non	Le CPS n'impose aucun lieu ; le prestataire est libre du data-center.
07/04/2025	02/2025 AUBB — Hébergement, infogérance & maintenance SIG + site	Agence Urbaine Berrechid-Benslimane	Hébergement cloud + TMA (5 ans)	Oui	« Serveurs en mode cloud hébergés et localisés au Maroc (Tier 3…) ».
24/04/2025	17-25-BGm — Refonte / maintenance portail	Établissement bancaire public	Refonte + MCO	Non	Serveur dédié mentionné, sans contrainte territoriale.
05/05/2025	20/AMDIE/2025 — Maintenance & évolutions site	Agence Marocaine de Développement des Investissements	TMA & évolutions	Non	Site maintenu sur plate-forme existante ; aucune clause de localisation.
21/05/2025	60-2025 — Refonte portail e-services (ministère)	Ministère (intitulé abrégé)	Refonte, migration, TMA	Non	Objectifs : UX, sécurité, dispo 99,9 %; localisation non évoquée.
11/06/2025	48-25 — Création site + hébergement	APDN / Wilaya Tanger-Tétouan-Al Hoceïma	Création site + hébergement (3 ans)	Non	Hébergement requis, mais pays non précisé.
24/06/2025	04/2025 AMEE — MEP + maintenance site	Agence Marocaine pour l'Efficacité Énergétique	Maintenance évolutive / corrective / préventive	Non	CPS décrit des serveurs AMEE, sans exigence « local Maroc ».
oct. 2025 (dossier)	01/2025 DIDH — Refonte site multilingue	Délégation Interministérielle aux Droits de l'Homme	Refonte, migration, hébergement, TMA	Non	Phase 4 : déploiement « sur l'environnement de production de la DIDH » sans contrainte territoriale.
17/07/1905	21/2025 — Portail communal Dar Bouazza	Commune de Dar Bouazza	Création + hébergement + audit	Oui	« Hébergement dans les serveurs de la Commune » ; sauvegarde locale hebdomadaire.