

La responsabilité des prestataires de services cloud face aux incidents de cybersécurité : les insuffisances du droit marocain à la lumière du droit comparé

Liability of cloud service providers for cybersecurity incidents: shortcomings of Moroccan law in the light of comparative law.

Auteur 1 : Abir OMRI..

Auteur 2 : Karim LGHMARI..

Auteur 3 : Soumaya AKKOUR..

Abir OMRI (doctorante)

Faculté des sciences politiques et juridiques settat

Université HASSAN I

Karim LAGHMARI (docteur)

Docteur en sciences juridiques

Soumaya AKKOUR (professeur de l'enseignement supérieur)

Faculté des sciences politiques et juridiques settat

Université HASSAN I

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

Conflit d'intérêts : Les auteurs ne signalent aucun conflit d'intérêts.

Pour citer cet article : OMRI .A, LAGHMARI .K & AKKOUR .S (2026) « La responsabilité des prestataires de services cloud face aux incidents de cybersécurité : les insuffisances du droit marocain à la lumière du droit comparé », African Scientific Journal « Volume 03, Num 38 » pp: 001 – 030.



DOI : 10.5281/zenodo.23435664.

Copyright © 2026 – ASJ



Résumé

Cet article analyse la responsabilité juridique des prestataires de services cloud face aux incidents de cybersécurité en droit marocain. À partir d'une étude doctrinale, normative et comparative, il confronte le Dahir des Obligations et des Contrats, les lois n° 53-05, 09-08 et 05-20, ainsi que le dispositif de qualification issu du décret n° 2-24-921 et de l'arrêté n° 3-17-25, aux standards européens et techniques pertinents. L'étude soutient que les obligations de cybersécurité relèvent principalement d'une obligation de moyens renforcée et montre que le modèle de responsabilité partagée demeure juridiquement incertain. Les principales limites identifiées concernent l'accès à la preuve numérique, l'établissement du lien de causalité, l'extraterritorialité, la portée des clauses limitatives et l'insuffisante articulation entre conformité, sanction et réparation. L'article conclut que le droit marocain offre des fondements mobilisables, mais reste fragmenté et partiellement inadapté aux spécificités du cloud. Il propose de clarifier les obligations des prestataires, d'aménager le régime probatoire, d'encadrer les clauses limitatives et d'articuler plus étroitement qualification, responsabilité et sanctions.

Mots-clés : Cloud computing - Cybersécurité - Responsabilité civile - Obligation de moyens renforcée - Responsabilité partagée - Preuve numérique - Droit marocain.

Abstract

This article examines the legal liability of cloud service providers for cybersecurity incidents under Moroccan law. Using a doctrinal, normative and comparative method, it assesses the Moroccan Code of Obligations and Contracts, Laws Nos. 53-05, 09-08 and 05-20, and the qualification framework introduced by Decree No. 2-24-921 and Order No. 3-17-25 against relevant European and technical standards. The study argues that cybersecurity duties are best characterised as enhanced duties of care and shows that the shared-responsibility model remains legally uncertain. The main weaknesses concern access to digital evidence, causation, extraterritoriality, liability limitation clauses, and the incomplete articulation between compliance, sanctions and compensation. It concludes that Moroccan law provides usable legal foundations but remains fragmented and only partially adapted to cloud-specific risks. The article recommends clarifying providers' duties, adjusting evidentiary rules, tightening control of liability clauses, and linking qualification requirements more directly to liability and enforcement mechanisms.

Keywords: Cloud computing - Cybersecurity - Civil liability - Enhanced duty of care - Shared responsibility - Digital evidence - Moroccan law.

Introduction

Au cours de la dernière décennie, la transformation numérique des organisations a profondément reconfiguré les modes de production, de gestion et de circulation de l'information. L'émergence du cloud computing s'inscrit dans cette dynamique en offrant aux entreprises et aux administrations des solutions externalisées de stockage, de traitement et de gestion des données, caractérisées par leur flexibilité, leur évolutivité et leur accessibilité. Ce modèle, fondé sur la mutualisation des ressources informatiques et l'accès à distance, constitue aujourd'hui un pilier essentiel de l'économie numérique.

Toutefois, cette externalisation des infrastructures informatiques s'accompagne d'une intensification significative des risques liés à la cybersécurité. Les incidents tels que les violations de données personnelles, les attaques par rançongiciel, les intrusions dans les systèmes d'information ou encore les indisponibilités de services illustrent la vulnérabilité croissante des environnements numériques¹. Dans ce contexte, la question de la sécurité des données et des systèmes devient un enjeu stratégique, tant pour les acteurs économiques que pour les autorités publiques.

Le cloud computing peut être défini comme un modèle de fourniture de services informatiques à la demande, permettant l'accès, via un réseau, à un ensemble de ressources configurables (serveurs, stockage, applications)². La cybersécurité renvoie, quant à elle, à l'ensemble des mesures techniques, organisationnelles et juridiques destinées à protéger les systèmes d'information contre les atteintes susceptibles de compromettre leur disponibilité, leur intégrité ou leur confidentialité. Enfin, la responsabilité juridique désigne l'obligation pour une personne de répondre des conséquences dommageables résultant de ses actes ou de ses manquements, qu'elle soit de nature contractuelle ou délictuelle.

Dans le contexte spécifique du cloud, la détermination de la responsabilité juridique des prestataires soulève des difficultés particulières. En effet, l'externalisation des services informatiques entraîne une dissociation entre le contrôle technique de l'infrastructure, assuré par le prestataire, et la

1 « Cloud computing: benefits, risks and recommendations for information security », European Union Agency for Cybersecurity, 2009 (révisé en 2012), https://www.enisa.europa.eu/sites/default/files/all_files/enisa-cloud-computing-final.pdf.

2 Peter Mell et Timothy Grance, The NIST Definition of Cloud Computing, no Special Publication 800-145, Septembre 2011 : 7 pages, <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>.

maîtrise fonctionnelle des données, qui demeure entre les mains du client. Cette dissociation complexifie l'identification des obligations respectives des parties et, par conséquent, la détermination de la responsabilité en cas d'incident de cybersécurité.

L'intérêt théorique du sujet réside dans la confrontation entre les catégories classiques du droit des obligations – notamment la distinction entre obligation de moyens et obligation de résultat – et les spécificités techniques du cloud computing, caractérisé par un environnement distribué, évolutif et marqué par une forte asymétrie d'information³⁴. Sur le plan pratique, l'enjeu est d'assurer une protection effective des utilisateurs et des clients des services cloud, tout en garantissant la sécurité juridique des prestataires et le développement de l'économie numérique.

En droit marocain, la responsabilité des prestataires de services cloud peut être appréhendée à travers les dispositions du Dahir des Obligations et des Contrats, qui constituent le socle du droit de la responsabilité civile, ainsi que par les textes spécifiques relatifs au numérique, notamment la loi n° 53-05 relative à l'échange électronique de données juridiques⁵, la loi n° 09-08 relative à la protection des données personnelles⁶ et la loi n° 05-20 relative à la cybersécurité⁷. Plus récemment, le décret n° 2-24-921 a encadré le recours à des prestataires cloud qualifiés par les entités et infrastructures d'importance vitale disposant de systèmes d'information ou de données sensibles ; l'arrêté n° 3-17-25 en a fixé le référentiel d'exigences⁸. La doctrine marocaine souligne cependant

3 Chris Reed, Internet Law: Text and Materials, Second edition (Cambridge University Press, 2004), https://assets.cambridge.org/97805216/05229/frontmatter/9780521605229_frontmatter.pdf.

4 Diane Rowland, Uta Kohl et Andrew Charlesworth, Information Technology Law, 5e éd., Routledge, 2016, DOI : 10.4324/9780203798522.

5 Loi n° 53-05 relative à l'échange électronique de données juridiques, promulguée par le dahir n° 1-07-129 du 30 novembre 2007.

6 Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, promulguée par le dahir n° 1-09-15 du 18 février 2009.

7 Loi n° 05-20 relative à la cybersécurité, promulguée par le dahir n° 1-20-69 du 25 juillet 2020.

8 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 ou de données sensibles, Bulletin officiel n° 7380 du 20 février 2025, p. 301 ; arrêté du Chef du gouvernement n° 3-17-25 du 7 safar 1447 (1er août 2025) fixant le référentiel des exigences de qualification des prestataires de services Cloud, Bulletin officiel n° 7432 du 21 août 2025, p. 2343.

que la multiplication des instruments de gouvernance numérique ne suffit pas, à elle seule, à garantir leur cohérence ni leur effectivité⁹¹⁰.

La présente recherche a pour objet d'apprécier la capacité du droit marocain à définir les obligations de sécurité des prestataires de services cloud et à organiser leur responsabilité civile lorsque survient un incident de cybersécurité. Elle poursuit trois objectifs complémentaires : qualifier juridiquement les obligations de prévention et de réaction, identifier les obstacles à l'imputation du dommage et à sa preuve, puis déterminer les adaptations normatives et contractuelles susceptibles de renforcer la protection des clients sans méconnaître les contraintes techniques des fournisseurs. La problématique se situe ainsi à l'intersection du droit des obligations, du droit de la cybersécurité et de la protection des données.

Dès lors, une interrogation centrale s'impose :

Dans quelle mesure le cadre juridique marocain est-il adapté à l'identification et à la sanction des manquements des prestataires de services cloud en matière de cybersécurité, et quelles évolutions normatives, inspirées du droit comparé, seraient nécessaires pour assurer une répartition équitable de la responsabilité juridique face au risque cyber ?

Hypothèses de recherche

H1 - Malgré les évolutions législatives et réglementaires récentes, le cadre juridique marocain demeure insuffisamment adapté à la qualification et à l'engagement de la responsabilité des prestataires de services cloud en matière de cybersécurité.

H2 - L'accès limité aux preuves numériques, l'asymétrie d'information, la pluralité des intervenants et l'implantation fréquente des prestataires à l'étranger constituent des obstacles majeurs à l'imputation technique et juridique des incidents.

H3 - Le renforcement des exigences de conformité et de qualification améliore la prévention, mais son effectivité demeure réduite par l'insuffisante articulation entre sanctions, réparation civile et clauses contractuelles limitatives de responsabilité.

9 Lamya Bassime, « L'évolution du cadre de gouvernance et de contrôle du numérique au Maroc », in Mélanges en l'honneur du Pr Abdellatif Komat, Éditions EMI, 2025, p. 317-340, DOI : 10.3917/emi.benni.2025.01.0317.

10 Kamal Lagtati et Dounia El Hamel, « La protection des données personnelles au Maroc à l'ère du numérique », Revue Internationale Burak des Études Juridiques et Économiques, vol. 1, n° 1, 2025, p. 236-248, DOI : 10.34874/PRSM.burak- vol1iss1.3353.

H4 - Une évolution inspirée du droit comparé permettrait de clarifier les obligations de sécurité, d'aménager la charge de la preuve et de mieux répartir les risques entre prestataire, client et sous-traitants.

Méthodologie

La recherche adopte une méthode doctrinale et normative. Le corpus principal comprend le Dahir des Obligations et des Contrats, les lois marocaines n° 53-05, 09-08 et 05-20, le décret n° 2-24-921, l'arrêté n° 3-17-25 et les instruments européens directement pertinents. Ces sources ont été retenues selon quatre critères : leur autorité juridique ou institutionnelle, leur lien direct avec la sécurité et la responsabilité dans le cloud, leur accessibilité vérifiable et, pour les instruments évolutifs, leur actualité.

Cette analyse est complétée par une revue documentaire structurée et systématisée de la doctrine, des normes techniques, des rapports institutionnels et des contentieux significatifs. La comparaison porte principalement sur l'Union européenne, la France et l'Allemagne, choisis en raison de la densité de leurs dispositifs de protection des données, de cybersécurité et de qualification des services cloud. La démarche est d'abord déductive, afin d'évaluer l'applicabilité des catégories du droit positif marocain, puis prospective, afin de formuler des propositions de réforme. L'étude ne prétend pas mesurer empiriquement la fréquence des incidents ou du contentieux ; elle apprécie la cohérence et l'effectivité potentielles des normes applicables.

Afin de renforcer la traçabilité du raisonnement, les instruments étudiés sont soumis à une grille d'analyse commune comportant cinq critères : le champ d'application personnel et matériel, le contenu des obligations préventives, les devoirs de documentation et de coopération, les conditions de mise en jeu de la responsabilité ainsi que les mécanismes de sanction et de réparation. Les affaires OVHcloud, Capital One et Blackbaud sont mobilisées comme illustrations contextualisées des difficultés d'imputation et non comme un échantillon représentatif. La comparaison demeure fonctionnelle : elle vise à repérer des solutions susceptibles d'inspirer le législateur marocain sans présupposer l'équivalence des régimes français, allemand, européen et marocain. La sélection documentaire, raisonnée plutôt qu'exhaustive, et l'absence de données empiriques constituent les principales limites de cette méthode juridique.

L'argumentation est structurée en deux parties. La première étudie le régime juridique de responsabilité des prestataires cloud à l'épreuve des incidents cyber : elle porte successivement sur la nature des obligations de sécurité et sur les conditions de mise en jeu de la responsabilité, notamment la preuve et la causalité (I). La seconde identifie les insuffisances du droit positif

marocain, avant d'examiner les enseignements du droit comparé et les propositions de consolidation d'un régime adapté aux risques du cloud (II). Cette organisation permet de passer du diagnostic juridique aux perspectives de réforme.

I. Régime juridique de responsabilité des prestataires cloud à l'épreuve des incidents cyber

Avant d'examiner les insuffisances du cadre juridique marocain, il convient, dans un premier temps, d'analyser les fondements et les modalités d'engagement de la responsabilité des prestataires de services cloud face aux incidents de cybersécurité. En effet, la compréhension du régime juridique applicable suppose d'identifier, d'une part, la nature des obligations qui pèsent sur ces prestataires, et, d'autre part, les conditions dans lesquelles leur responsabilité peut être engagée en cas de défaillance sécuritaire. Cette analyse est d'autant plus essentielle que les spécificités techniques du cloud computing, marquées par une forte asymétrie d'information et une pluralité d'intervenants, viennent complexifier l'application des mécanismes classiques du droit de la responsabilité. Dès lors, il apparaît nécessaire de s'interroger, dans un premier temps, sur la qualification juridique des obligations de cybersécurité, avant d'examiner, dans un second temps, les conditions d'engagement de la responsabilité du prestataire.

1 – Nature juridique des obligations de cybersécurité du prestataire cloud

1.1 – Qualification des obligations : moyens, résultat ou obligation renforcée

La détermination de la nature juridique des obligations pesant sur les prestataires de services cloud constitue une question centrale dans l'analyse de leur responsabilité. En effet, la qualification de l'obligation de cybersécurité conditionne directement le régime de preuve applicable ainsi que les chances d'indemnisation du client victime en cas d'incident.

Traditionnellement, le droit des obligations distingue entre l'obligation de moyens, qui impose au débiteur de mettre en œuvre toutes les diligences nécessaires sans garantir un résultat déterminé, et l'obligation de résultat, qui engage sa responsabilité dès lors que le résultat promis n'est pas atteint, sauf cas de force majeure. Cette distinction, bien établie en droit civil, apparaît toutefois difficilement transposable en l'état aux environnements numériques complexes que constitue le cloud computing.

En effet, les prestataires cloud s'engagent, dans le cadre contractuel, à assurer un ensemble de garanties relatives à la sécurité, à la disponibilité et à la confidentialité des données. Ces engagements sont généralement formalisés à travers des accords de niveau de service (Service Level Agreements – SLA), qui fixent des standards de performance et des obligations de sécurité. À première vue, certaines de ces obligations, notamment celles relatives à la disponibilité des

services, pourraient être assimilées à des obligations de résultat, dans la mesure où elles sont souvent exprimées en termes quantifiés (taux de disponibilité, délais de rétablissement).

Toutefois, une telle qualification doit être nuancée. La cybersécurité se caractérise par une incertitude intrinsèque liée à l'évolution constante des menaces et à la sophistication des attaques¹¹. Dans ce contexte, imposer au prestataire une obligation de résultat absolue en matière de sécurité reviendrait à lui faire supporter un risque excessif, difficilement conciliable avec la réalité technique des systèmes d'information.

C'est pourquoi une partie importante de la doctrine considère que les obligations de cybersécurité relèvent d'une catégorie intermédiaire, qualifiée d'obligation de moyens renforcée¹²¹³. Cette qualification implique que le prestataire doit mettre en œuvre toutes les mesures techniques et organisationnelles appropriées, conformément aux standards de l'état de l'art, aux exigences réglementaires et aux bonnes pratiques du secteur. Il ne s'agit donc pas de garantir l'absence totale d'incident, mais de démontrer un niveau élevé de diligence.

Cette approche trouve un fondement dans le droit marocain du numérique. En effet, la loi n° 09-08 impose aux responsables de traitement et à leurs sous-traitants des obligations de sécurité destinées à protéger les données personnelles contre toute atteinte¹⁴. De même, la loi n° 05-20 relative à la cybersécurité consacre une logique de gestion des risques, impliquant la mise en place de dispositifs de protection adaptés à la sensibilité des systèmes d'information. Le décret n° 2-24-921, applicable au recours au cloud par certaines entités et infrastructures d'importance vitale manipulant des systèmes ou données sensibles, renforce cette exigence en imposant le recours à des prestataires qualifiés. L'arrêté du Chef du gouvernement n° 3-17-25, qui fixe le référentiel des exigences de qualification, donne un contenu concret à ces standards. C'est ainsi qu'un juge saisi d'un litige y trouvera des repères objectifs pour apprécier la diligence du prestataire.

11 Ali Dehghantanha et al., éd., *Cyber Threat Intelligence*, vol. 70, *Advances in Information Security* (Springer International Publishing, 2018), <https://doi.org/10.1007/978-3-319-73951-9>.

12 W. Kuan Hon, Christopher Millard et Ian Walden, « Who is responsible for "personal data" in cloud computing? The cloud of unknowing, Part 2 », *International Data Privacy Law*, vol. 2, n° 1, 2012, p. 3-18, DOI : 10.1093/idpl/ipr025.

13 Siani Pearson et George Yee, éd., *Privacy and Security for Cloud Computing*, *Computer Communications and Networks* (Springer, 2013), <https://doi.org/10.1007/978-1-4471-4189-1>.

14 Art. 23 de la loi n° 09-08, cité supra.

Dès lors, la qualification d'obligation de moyens renforcée apparaît comme la plus pertinente, en ce qu'elle permet de concilier les exigences de protection des utilisateurs avec les contraintes techniques inhérentes au cloud computing. Toutefois, cette qualification n'est pas sans conséquence sur le plan probatoire : elle implique que la charge de la preuve du manquement pèse en principe sur le client, ce qui soulève des difficultés importantes en pratique.

En définitive, la qualification juridique des obligations de cybersécurité révèle les limites des catégories traditionnelles du droit des obligations face aux mutations technologiques. Elle invite à repenser les mécanismes de responsabilité à la lumière des spécificités du numérique, en intégrant notamment les enjeux liés à la preuve et à l'asymétrie d'information.

À cet égard, l'analyse technique de la prestation ne peut être dissociée de sa qualification juridique. Jansen et Grance (NIST SP 800-144, 2011) soulignent les risques liés à l'externalisation de l'infrastructure et à la perte de maîtrise directe de certains contrôles de sécurité ; Mather, Kumaraswamy et Latif (2009) mettent pareillement en avant l'importance de l'audit, de la gouvernance et des engagements contractuels dans la détermination de la diligence attendue du fournisseur.

1.2 – Modèle de responsabilité partagée et ses implications juridiques : répartition des rôles entre prestataire et client

Le fonctionnement des services de cloud computing repose sur un principe fondamental, communément désigné sous l'expression de modèle de responsabilité partagée. Ce modèle implique une répartition des obligations de sécurité entre le prestataire de services cloud et le client utilisateur, en fonction du type de service fourni (Infrastructure as a Service, Platform as a Service ou Software as a Service)¹⁵¹⁶. Si ce mécanisme présente un intérêt opérationnel évident, il soulève néanmoins d'importantes difficultés juridiques en matière d'imputation des responsabilités.

En principe, le prestataire cloud est responsable de la sécurité de l'infrastructure sous-jacente, incluant les centres de données, les serveurs, les réseaux et les mécanismes de virtualisation. Il lui incombe, à ce titre, de mettre en place des mesures techniques et organisationnelles garantissant la

15 S. Subashini et V. Kavitha, « A survey on security issues in service delivery models of cloud computing », *Journal of Network and Computer Applications* 34, no 1 (2011): 1-11, <https://doi.org/10.1016/j.jnca.2010.07.006>.

16 Hassan Takabi et al., « Security and Privacy Challenges in Cloud Computing Environments », *IEEE Security & Privacy* 8, no 6 (2010): 24-31, <https://doi.org/10.1109/MSP.2010.186>.

disponibilité, l'intégrité et la confidentialité des données hébergées¹⁷. Le client, quant à lui, demeure responsable de la gestion des accès, de la configuration des services, ainsi que de la protection des données qu'il traite ou stocke sur la plateforme.

Toutefois, cette répartition théorique des responsabilités se révèle, en pratique, particulièrement délicate à mettre en œuvre. En effet, les frontières entre les obligations du prestataire et celles du client sont souvent imprécises, notamment en raison de la complexité technique des environnements cloud et de l'opacité des architectures utilisées. Cette situation engendre une incertitude juridique quant à l'identification du responsable en cas d'incident de cybersécurité.

En outre, les contrats de services cloud, et en particulier les accords de niveau de service (SLA), tendent à formaliser cette répartition des responsabilités. Néanmoins, ces instruments contractuels sont généralement rédigés de manière unilatérale par les prestataires et peuvent contenir des clauses ambiguës ou déséquilibrées, limitant la portée des obligations qui leur incombent¹⁸. Il en résulte un risque de dilution de la responsabilité, dans la mesure où chaque partie peut tenter de rejeter la faute sur l'autre en cas de défaillance.

Cette problématique est accentuée par la multiplicité des intervenants dans l'écosystème cloud. En effet, un prestataire peut lui-même recourir à des sous-traitants ou à d'autres fournisseurs d'infrastructure, créant ainsi une chaîne complexe de responsabilités. Dans un tel contexte, l'identification de l'auteur du manquement devient particulièrement difficile, ce qui complique l'engagement de la responsabilité juridique.

Par ailleurs, le modèle de responsabilité partagée soulève des interrogations quant à sa compatibilité avec les exigences du droit marocain, notamment en matière de protection des données personnelles. La loi n° 09-08 impose des obligations spécifiques aux responsables de traitement et à leurs sous-traitants, ce qui suppose une clarification précise des rôles de chacun. Or, le caractère parfois flou du modèle cloud peut entrer en tension avec ces exigences. À cet égard, plusieurs propositions doctrinales préconisent une réforme de la loi n° 09-08 afin de rapprocher le droit marocain des standards européens, notamment par le renforcement des pouvoirs de sanction de la commission nationale de contrôle de la protection des données à caractère personnel

17 Normes ISO/IEC 27001 (management de la sécurité de l'information), ISO/IEC 27017:2015 (mesures de sécurité applicables aux services cloud) et ISO/IEC 27018:2019 (protection des données personnelles dans le cloud public).

18 Christopher Millard, éd., *Cloud Computing Law*, Second Edition (Oxford University Press, 2021), <https://global.oup.com/academic/product/cloud-computing-law-9780198716662?cc=ma&lang=en&#>.

(CNDP)¹⁹, l'introduction d'amendes administratives proportionnées au chiffre d'affaires et la consécration d'un régime de responsabilité plus explicite entre responsable du traitement et sous-traitant. Les analyses doctrinales nationales consacrées à l'alignement du droit marocain sur les standards européens confirment l'intérêt d'une telle clarification²⁰.

Dès lors, si le modèle de responsabilité partagée constitue un outil fonctionnel indispensable à l'exploitation des services cloud, il apparaît également comme une source d'insécurité juridique. Cette situation appelle à une meilleure clarification normative des obligations respectives des acteurs, afin d'éviter les situations de dilution de responsabilité et de garantir une protection effective des utilisateurs.

Le tableau suivant explicite les principales zones de contrôle. Il ne constitue pas une règle légale uniforme : la répartition effective doit être vérifiée au regard du contrat, de l'architecture déployée et des exigences réglementaires applicables.

Tableau 1 — Répartition indicative des obligations de sécurité selon le modèle cloud

Dimension de sécurité	IaaS	PaaS	SaaS
Infrastructure physique et réseau hôte	Prestataire	Prestataire	Prestataire
Sécurité du système d'exploitation	Client, selon service	Généralement prestataire	Généralement prestataire
Applications et mises à jour	Client	Responsabilités partagées	Généralement prestataire
Identités, habilitations, données	Client et prestataire selon fonction	Partagée	Partagée
Journaux, notification, coopération probatoire	Répartition contractuelle et légale	Répartition contractuelle et légale	Répartition contractuelle et légale

Source : synthèse élaborée à partir de Mell et Grance (2011), Jansen et Grance (2011) et Subashini et Kavitha (2011).

¹⁹ « Commission nationale de contrôle de la protection des données à caractère personnel », CNDP, <https://www.cndp.ma/>.

²⁰ Najoua Rouini et Amira El Aidouni, « Analyse comparative de la réglementation sur la protection des données à caractère personnel entre le Maroc et l'Union européenne », Revue de Droit Civil, Économique et Comparé, vol. 4, n° 2, 2023, DOI : 10.34874/PRSM.rdcec-vol4iss2.45030.

2 – Conditions d’engagement de la responsabilité du prestataire

2.1 – Difficultés probatoires face à l’incident cyber : accès aux preuves forensiques et asymétrie d’information

L’engagement de la responsabilité du prestataire de services cloud suppose, conformément aux principes généraux du droit civil marocain, la réunion de trois éléments cumulatifs : une faute, un dommage et un lien de causalité²¹. Toutefois, en matière de cybersécurité, la mise en œuvre de ces conditions se heurte à des difficultés probatoires spécifiques, liées à la nature technique et immatérielle des incidents.

La première difficulté réside dans l’accès aux éléments de preuve. En effet, les données techniques nécessaires à l’analyse d’un incident cyber – telles que les journaux de connexion (logs), les traces d’activité, les rapports d’audit ou encore les données forensiques – sont, dans la majorité des cas, détenues exclusivement par le prestataire cloud. Cette situation crée une asymétrie informationnelle structurelle entre le prestataire et le client, ce dernier se trouvant dans l’incapacité matérielle de démontrer l’origine du dysfonctionnement ou du manquement allégué.

Cette asymétrie est d’autant plus problématique que le droit marocain repose, en principe, sur une répartition classique de la charge de la preuve, selon laquelle il appartient au demandeur d’établir les faits qu’il invoque²². Or, dans le contexte du cloud computing, cette exigence peut conduire à un déséquilibre procédural au détriment du client victime, réduisant ainsi l’effectivité du droit à réparation.

Par ailleurs, la complexité technique des incidents de cybersécurité constitue un obstacle supplémentaire. Les attaques informatiques peuvent résulter d’une combinaison de facteurs - vulnérabilité logicielle, erreur de configuration, défaillance humaine ou intrusion externe - rendant difficile l’identification précise de leur cause. La preuve du manquement suppose souvent une expertise technique approfondie, dont le coût et la complexité peuvent dissuader les victimes d’agir. Cette expertise doit reposer sur des éléments fiables : l’identification, la collecte, l’acquisition et la conservation des preuves numériques obéissent à des exigences strictes de traçabilité et

21 « Code des obligations et des contrats (promulgué par Dahir du 9 Ramadan 1331 (12 août 1913), et modifié par la loi n° 24-09) », Maroc, <https://www.wipo.int/wipolex/fr/legislation/details/14741>. Voir les articles 77 et 78 (responsabilité délictuelle) et les articles 263 et suivants (conséquences de l’inexécution des obligations contractuelles).

22 Idem. Voir l’article 399 (preuve de l’obligation devant être faite par celui qui s’en prévaut)

d'intégrité²³. La doctrine marocaine rappelle, à cet égard, que la recevabilité et la force probante de la preuve numérique dépendent autant de son fondement juridique que de la préservation de la chaîne de conservation²⁴.

En outre, l'intervention de multiples acteurs dans l'écosystème cloud – prestataires d'infrastructure, fournisseurs de services, sous-traitants – contribue à diluer les responsabilités et complique davantage la recherche de la preuve. L'identification de l'auteur du manquement devient alors un exercice particulièrement délicat, susceptible d'entraver l'engagement effectif de la responsabilité. Dès lors, ces difficultés probatoires invitent à repenser les mécanismes traditionnels de la preuve en matière de responsabilité civile, en envisageant notamment des aménagements tels que l'allègement de la charge de la preuve ou l'instauration de présomptions de responsabilité à la charge du prestataire, inspirées des évolutions observées en droit comparé.

Sur le plan opérationnel, le référentiel NIST SP 800-61, révision 3 (2025), met en évidence l'intérêt de préparer la réponse à incident, d'identifier les rôles, de documenter les événements et de conserver les éléments nécessaires aux investigations. Un tel cadre technique ne crée pas, à lui seul, une présomption de responsabilité en droit marocain, mais offre des critères objectivables pour apprécier la diligence et structurer les demandes de production de preuves.

Tableau 2 — Éléments probatoires utiles après un incident de cybersécurité

Élément	Détenteur probable	Utilité pour le contentieux	Précaution de conservation
Journaux d'accès et d'authentification	Prestataire et/ou client	Identifier accès, chronologie et périmètre	Horodatage fiable, intégrité, traçabilité
Rapports d'audit et tests de sécurité	Prestataire / auditeur	Évaluer le respect du standard de diligence	Versionnement, confidentialité, mandat
Dossiers d'incident et alertes	Prestataire / équipe de réponse	Établir mesures prises et délais	Chaîne de conservation, registre des actions
Contrat, SLA et matrice de responsabilités	Parties contractantes	Imputer les obligations et vérifier les exclusions	Conserver versions opposables

²³ Norme ISO/IEC 27037 : 2012 (lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques).

²⁴ Anouar Abou El Jaouad, « La preuve numérique à l'épreuve de la cybercriminalité en droit marocain », Revue Droit & Société, n° 11, octobre 2023, DOI : 10.5281/zenodo.10054215.

Justificatifs du préjudice	Client / tiers	Quantifier la perte et discuter la causalité	Pièces datées et expertise contradictoire
----------------------------	----------------	--	---

Source : synthèse des exigences probatoires évoquées dans l'article, de la norme ISO/IEC 27037:2012 et du NIST SP 800-61 Rev. 3 (2025).

2.2 – Appréciation du manquement et du lien de causalité : caractérisation de la faute et imputation du préjudice

Au-delà des difficultés probatoires, l'engagement de la responsabilité du prestataire cloud suppose également une appréciation rigoureuse du manquement et du lien de causalité entre celui-ci et le dommage subi.

La caractérisation de la faute repose sur l'identification d'un manquement aux obligations de sécurité pesant sur le prestataire. Toutefois, dans un environnement technologique en constante évolution, la détermination du standard de diligence applicable demeure incertaine. La référence à « l'état de l'art » ou aux « bonnes pratiques » du secteur, fréquemment utilisée, présente un caractère évolutif et parfois imprécis, ce qui rend l'appréciation judiciaire délicate.

Par ailleurs, la qualification de l'obligation de cybersécurité comme obligation de moyens renforcée implique que la faute ne peut être retenue qu'en cas de démonstration d'un défaut de diligence caractérisé. Il ne suffit pas de constater la survenance d'un incident pour engager la responsabilité du prestataire ; encore faut-il établir que celui-ci n'a pas mis en œuvre les mesures de sécurité appropriées.

Le lien de causalité constitue une autre difficulté majeure. En effet, l'imputation du dommage à un manquement précis du prestataire est souvent compliquée par la multiplicité des causes possibles. Un incident de cybersécurité peut résulter d'une défaillance du prestataire, mais également d'une mauvaise configuration imputable au client, d'une attaque externe imprévisible ou d'un dysfonctionnement d'un tiers intervenant.

Cette pluralité des causes soulève la question de la répartition de la responsabilité entre les différents acteurs. En l'absence de règles claires, le juge est amené à procéder à une appréciation au cas par cas, ce qui peut engendrer une insécurité juridique.

Enfin, la question de l'extraterritorialité vient complexifier davantage l'analyse. Dans de nombreux cas, les prestataires cloud sont établis à l'étranger, ce qui soulève des difficultés relatives à la compétence juridictionnelle, au droit applicable et à l'exécution des décisions de justice marocaines. Cette dimension internationale du cloud constitue un obstacle supplémentaire à l'effectivité de la responsabilité. L'adhésion du Maroc à la Convention de Budapest sur la

cybercriminalité²⁵ ouvre des canaux de coopération pour la collecte transfrontalière de la preuve électronique. Elle ne règle en revanche ni la loi applicable à la responsabilité civile du prestataire étranger, ni l'exécution des décisions marocaines contre des opérateurs non établis au Royaume. L'affaire Microsoft Ireland, dans laquelle l'éditeur américain refusait de remettre au département de justice américain des courriels stockés en Irlande, a montré l'ampleur du défi²⁶. Dans ce cadre, le Cloud Act de 2018 a répondu de manière régaliennne à ce problème, en permettant aux autorités des États-Unis d'accéder aux données détenues par les fournisseurs américains où qu'elles soient stockées²⁷.

Ainsi, l'appréciation du manquement et du lien de causalité met en lumière les limites des mécanismes classiques du droit de la responsabilité face aux spécificités des incidents de cybersécurité. Elle souligne la nécessité d'une adaptation du cadre juridique afin de mieux prendre en compte la complexité technique et organisationnelle des services cloud.

II. Limites du droit positif marocain et perspectives d'évolution

Si l'analyse du régime juridique applicable aux prestataires de services cloud met en évidence l'existence de fondements normatifs permettant, en théorie, d'engager leur responsabilité en cas d'incident de cybersécurité, elle révèle également les limites structurelles du cadre juridique marocain face aux spécificités techniques et organisationnelles du cloud computing. En effet, la complexité des environnements numériques, la dématérialisation des supports, la multiplicité des acteurs impliqués ainsi que la dimension transfrontalière des services cloud mettent à l'épreuve les catégories classiques du droit de la responsabilité.

Dans ce contexte, le droit positif marocain apparaît, à bien des égards, insuffisamment adapté pour appréhender de manière cohérente les enjeux liés à la cybersécurité dans les environnements externalisés. Cette insuffisance tient notamment au caractère fragmenté des sources normatives, à

25 « Le Maroc adhère à la Convention de Budapest sur la cybercriminalité et à son Protocole sur la xénophobie et le racisme - Cybercriminalité - www.coe.int », Cybercriminalité, consulté le 10 juillet 2023, https://www.coe.int/fr/web/cybercrime/cybersouth-activities/-/asset_publisher/evi3rDpsvYdT/content/morocco-joins-the-budapest-convention-on-cybercrime-and-becomes-it-s-60th-member-.

26 « Microsoft v. United States, No. 14-2985 (2d Cir. 2016) », Justia Law, <https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html>.

27 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018), codifié notamment à 18 U.S.C. § 2713.

l'absence de qualification juridique claire des obligations pesant sur les prestataires cloud, ainsi qu'aux difficultés liées à l'encadrement des mécanismes contractuels et à la mise en œuvre effective de la responsabilité.

Dès lors, il convient d'examiner, dans un premier temps, les insuffisances du cadre juridique national à travers l'analyse des instruments existants et de leurs lacunes (Section 1), avant d'envisager, dans un second temps, les voies de consolidation d'un régime de responsabilité plus adapté, inspiré notamment des enseignements du droit comparé (Section 2).

1 – Adaptation insuffisante du cadre juridique national

1.1 – Instruments existants et leurs lacunes : DOC, lois spéciales et décret relatif aux prestataires cloud

Le droit marocain encadrant la responsabilité des prestataires de services cloud repose sur un ensemble de textes de nature hétérogène, comprenant à la fois les dispositions générales du Dahir des Obligations et des Contrats, ainsi que des textes spéciaux relatifs au numérique, notamment la loi n° 09-08 relative à la protection des données personnelles, la loi n° 05-20 relative à la cybersécurité et, plus récemment, le décret n° 2-24-921 organisant, pour certaines entités et infrastructures d'importance vitale, le recours à des prestataires de services cloud qualifiés.

Le Dahir des Obligations et des Contrats constitue le socle du droit de la responsabilité civile au Maroc. Il pose les principes fondamentaux de la responsabilité contractuelle et délictuelle, fondés sur la faute, le dommage et le lien de causalité. Toutefois, ces dispositions, élaborées dans un contexte économique et technologique radicalement différent, ne prennent pas en considération les spécificités des environnements numériques, et en particulier celles du cloud computing. L'absence de dispositions spécifiques relatives aux obligations de sécurité informatique ou à la gestion des risques cyber limite ainsi la portée opérationnelle de ces règles dans le contexte des services cloud. Les lois spéciales relatives au numérique apportent, quant à elles, des éléments de réponse partiels. La loi n° 09-08 impose aux responsables de traitement et à leurs sous-traitants des obligations de sécurité visant à protéger les données personnelles contre tout accès non autorisé ou toute altération. De même, la loi n° 05-20 introduit un cadre de gouvernance de la cybersécurité fondé sur la gestion des risques et la protection des systèmes d'information d'importance vitale. Toutefois, ces textes ne visent pas spécifiquement les prestataires cloud en tant que tels, et ne permettent pas de définir de manière précise l'étendue de leurs obligations en cas d'incident.

Le dispositif existant n'est toutefois pas dépourvu de sanctions. Les articles 58 et 61 de la loi n° 09-08 punissent notamment l'absence de mesures de sécurité et le fait, même par négligence, de

faciliter un usage abusif ou une communication non autorisée de données : les peines prévues peuvent atteindre un an d'emprisonnement et 200 000 dirhams d'amende²⁸. Ces sanctions pénales fixes contribuent à la répression des manquements, mais elles ne constituent ni un régime administratif gradué en fonction de la taille de l'opérateur, ni un mécanisme autonome de réparation du dommage subi par le client. Cette dissociation confirme la faiblesse de l'articulation entre conformité, sanction et responsabilité civile.

L'adoption du décret n° 2-24-921 relatif au recours à des prestataires de services cloud qualifiés dans son champ d'application constitue une avancée notable, en ce qu'il introduit des exigences techniques et organisationnelles visant à renforcer la sécurité des services proposés. Néanmoins, ce dispositif demeure principalement orienté vers une logique de certification et de conformité, sans apporter de réponses suffisantes aux questions relatives à l'engagement de la responsabilité en cas de manquement. Sa mise en œuvre effective dépendra de l'appropriation du référentiel fixé par l'arrêté n° 3-17-25 et, surtout, de son articulation avec les régimes de responsabilité de droit commun.

Par ailleurs, l'articulation entre ces différentes sources normatives apparaît insuffisamment claire. L'absence de coordination entre le droit commun de la responsabilité et les régimes spéciaux du numérique engendre une certaine insécurité juridique, tant pour les prestataires que pour les utilisateurs. Cette fragmentation du cadre juridique nuit à la lisibilité du droit applicable et complique son application pratique. La doctrine nationale consacrée à la gouvernance et au contrôle du numérique formule un constat convergent : l'accumulation de textes sectoriels appelle un effort d'harmonisation, de coordination institutionnelle et de lisibilité normative²⁹.

Ainsi, si le droit marocain offre un ensemble de fondements juridiques mobilisables, il demeure marqué par une insuffisance structurelle dans l'appréhension des spécificités du cloud computing, ce qui limite son efficacité en matière de gestion des incidents de cybersécurité.

Le rapprochement des textes met en évidence une différence de fonction entre la réparation de droit commun, les obligations sectorielles de prévention et le contrôle de conformité. Leur coexistence

²⁸ Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, art. 58 et 61 : emprisonnement de trois mois à un an et amende de 20 000 à 200 000 dirhams, ou l'une de ces deux peines seulement, selon le manquement considéré.

²⁹ Lamya Bassime, « L'évolution du cadre de gouvernance et de contrôle du numérique au Maroc », in Mélanges en l'honneur du Pr Abdellatif Komat, Éditions EMI, 2025, p. 317-340, DOI : 10.3917/emi.benni.2025.01.0317.

ne doit donc pas être confondue avec l'existence d'un régime autonome de responsabilité civile propre au cloud.

Tableau 3 — Portée et limites des principaux instruments marocains

Instrument	Apport au traitement du risque cloud	Limite relevée
Dahir des obligations et des contrats	Fondement de la responsabilité contractuelle et délictuelle	Preuve et causalité difficiles dans les systèmes distribués
Loi n° 09-08	Obligations relatives à la sécurité des données personnelles ; sanctions	Articulation incomplète avec l'indemnisation du client
Loi n° 05-20	Prévention et gouvernance de la cybersécurité pour les entités concernées	Champ et mécanismes distincts d'un droit commun du cloud
Décret n° 2-24-921 et arrêté n° 3-17-25	Qualification et exigences applicables dans le champ défini	Ne créent pas à eux seuls un régime général de réparation
Loi n° 53-05	Cadre de l'échange électronique et de la preuve selon son objet	Réponse non spécifique à l'accès aux traces forensiques

Source : lecture croisée des textes normatifs cités dans l'article ; tableau analytique, sans assimilation des champs d'application.

1.2 – Clauses limitatives de responsabilité : validité et opposabilité des plafonds d'indemnisation et exclusions en cas de risque cyber

Les contrats de services cloud, et plus particulièrement les accords de niveau de service (Service Level Agreements – SLA), comportent quasi systématiquement des clauses limitatives ou exonératoires de responsabilité. Ces stipulations contractuelles visent à encadrer, voire à restreindre, l'étendue de la responsabilité du prestataire en cas de défaillance, notamment en plafonnant les montants d'indemnisation ou en excluant certains types de préjudices, tels que les pertes indirectes, les pertes de données ou les atteintes à la réputation.

En droit marocain, la validité de ces clauses s'apprécie au regard des principes généraux du droit des obligations. En vertu du Dahir des Obligations et des Contrats, les parties disposent d'une liberté contractuelle leur permettant d'aménager les conditions de la responsabilité, sous réserve du respect de certaines limites. Ainsi, les clauses limitatives de responsabilité sont en principe

admises, sauf lorsqu'elles portent atteinte à une obligation essentielle du contrat, ou lorsqu'elles visent à exonérer une partie en cas de faute lourde ou de dol³⁰.

Dans le contexte des services cloud, la question de la validité de ces clauses revêt une acuité particulière. En effet, les obligations de sécurité, de confidentialité et de disponibilité des données constituent le cœur même de la prestation fournie par le prestataire cloud. Dès lors, toute clause ayant pour effet de vider de sa substance ces obligations pourrait être considérée comme nulle ou inopposable.

Par ailleurs, la généralisation des clauses limitatives de responsabilité dans les contrats cloud pose la question de l'équilibre contractuel. Ces contrats sont souvent des contrats d'adhésion, dont les stipulations sont imposées par le prestataire sans réelle possibilité de négociation pour le client, en particulier lorsque celui-ci est une petite ou moyenne entreprise. Il en résulte un déséquilibre structurel entre les parties, susceptible d'affecter la protection juridique du client.

En outre, l'application de ces clauses dans le contexte des incidents de cybersécurité soulève des difficultés spécifiques. D'une part, les prestataires invoquent fréquemment des clauses d'exclusion liées à des événements assimilés à des cas de force majeure³¹, tels que les cyberattaques sophistiquées. D'autre part, la qualification de faute lourde ou de manquement grave, susceptible d'écarter l'application de ces clauses, demeure délicate à établir en pratique, en raison des difficultés probatoires évoquées précédemment. Dans ce cadre, le contentieux ayant suivi l'incendie du centre de données du prestataire européen OVHcloud à Strasbourg, en mars 2021, illustre concrètement ces tensions. Le tribunal de commerce de Lille Métropole a en effet écarté des clauses limitatives qui vidaient de sa substance l'obligation essentielle de sauvegarde du prestataire³². Dans le même ordre d'idée, l'attaque par rançongiciel subie en 2020 aux États-Unis par la société Blackbaud, éditeur de solutions SaaS pour le secteur associatif, a donné lieu à une procédure

30 « Code des obligations et des contrats (promulgué par Dahir du 9 Ramadan 1331 (12 août 1913), et modifié par la loi n° 24-09) ». Voir l'article 232 (On ne peut stipuler d'avance qu'on ne sera pas tenu de son dol ou de sa faute lourde).

31 Idem. Voir les articles 268 et 269 (définition de la force majeure).

32 Legalis | L'actualité du droit des nouvelles technologies | Tribunal de commerce de Lille Métropole, jugement du 26 janvier 2023, s. d., <https://www.legalis.net/jurisprudences/tribunal-de-commerce-de-lille-metropole-jugement-du-26-janvier-2023/>.

fédérale consolidée³³, puis à un règlement de 49,5 millions de dollars avec les procureurs généraux de quarante-neuf États ; dans le cadre de cet accord, Blackbaud s'est engagée à améliorer ses programmes de cybersécurité pour protéger les données des utilisateurs³⁴. Quant à l'affaire Capital One, la violation de données de 2019 a exploité une configuration défaillante dans l'environnement cloud de la banque³⁵. Des actions civiles ont visé Capital One et Amazon³⁶, mais la sanction administrative de 80 millions de dollars prononcée par l'Office of the Comptroller of the Currency a été fondée sur les insuffisances de la banque dans l'évaluation des risques et les contrôles précédant sa migration vers le cloud³⁷. Cet exemple montre que le modèle de responsabilité partagée n'entraîne ni l'immunité du fournisseur ni sa responsabilité automatique : l'imputation dépend du périmètre de contrôle, des obligations contractuelles et des preuves techniques relatives à la configuration et à la vulnérabilité exploitées.

Il convient également de prendre en considération les exigences issues des lois spéciales du numérique. La loi n° 09-08 relative à la protection des données personnelles impose des obligations de sécurité qui présentent, dans certains cas, un caractère impératif, notamment en ce qui concerne la protection des données sensibles. De même, la loi n° 05-20 relative à la cybersécurité impose des exigences spécifiques aux infrastructures d'importance vitale. Ces dispositions peuvent limiter la portée des clauses contractuelles, en interdisant toute dérogation aux obligations de sécurité imposées par la loi.

33 « In Re Blackbaud, Inc., Customer Data Breach Litigation », Cohen Milstein, 15 mars 2021, <https://www.cohenmilstein.com/case-study/re-blackbaud-inc-customer-data-breach-litigation/>.

34 « Blackbaud Resolves Multi-State Attorneys General Investigation of 2020 Security Incident », Blackbaud, s. d., <https://www.blackbaud.com/newsroom/article/blackbaud-resolves-multi-state-attorneys-general-investigation-of-2020-security-incident>.

35 Shaharyar Khan et al., A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned, ACM Transactions on Privacy and Security 26, no 1 (2022): 3:1-3:29, <https://doi.org/10.1145/3546068>.

36 « In Re: Capital One Customer Data Security Breach Litigation, 1:19-Md-02915 - CourtListener.Com », CourtListener, <https://www.courtlistener.com/docket/16328328/in-re-capital-one-customer-data-security-breach-litigation/>.

37 Office of the Comptroller of the Currency, « OCC Assesses \$80 Million Civil Money Penalty Against Capital One », News Release 2020-101, 6 août 2020 ; Consent Order for the Assessment of a Civil Money Penalty, AA-EC-2020-63.

Dès lors, les clauses limitatives de responsabilité apparaissent comme un instrument contractuel ambivalent. Si elles répondent à une logique économique de maîtrise des risques pour les prestataires, elles peuvent également réduire l'effectivité de la protection des clients en cas d'incident de cybersécurité. Cette tension entre liberté contractuelle et impératif de sécurité juridique invite à un encadrement plus strict de ces clauses, afin de garantir un équilibre entre les intérêts en présence.

2 – Voies de consolidation d'un régime de responsabilité adapté

2.1 – Enseignements du droit comparé : RGPD, régulation de la cybersécurité et modèles européens

L'analyse du droit comparé, et en particulier du droit de l'Union européenne, met en évidence des mécanismes juridiques plus avancés en matière d'encadrement de la responsabilité des acteurs du numérique face aux risques cybernétiques. Ces instruments offrent des pistes pertinentes pour repenser le cadre juridique marocain.

En premier lieu, le Règlement général sur la protection des données (RGPD)³⁸ consacre une approche renforcée de la responsabilité des acteurs intervenant dans le traitement des données personnelles. Il impose aux responsables de traitement et à leurs sous-traitants des obligations strictes en matière de sécurité, fondées sur le principe de « responsabilité » (accountability). Cette logique implique que les acteurs doivent non seulement respecter les règles, mais également être en mesure de démontrer leur conformité, notamment par la mise en place de mesures techniques et organisationnelles appropriées.

Par ailleurs, le RGPD introduit des mécanismes facilitant l'engagement de la responsabilité, tels que la responsabilité conjointe entre acteurs et l'instauration de sanctions administratives significatives. Cette approche contribue à renforcer l'effectivité du droit en matière de protection des données.

En matière de données personnelles, les lignes directrices 07/2020 du Comité européen de la protection des données (version finale du 7 juillet 2021) éclairent la distinction fonctionnelle entre responsable de traitement et sous-traitant. Elles rappellent, dans un cadre comparatif, que la

³⁸ 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), 119 OJ L (2016), <http://data.europa.eu/eli/reg/2016/679/oj>. Voir les articles 28, 32, 82 et 83.

répartition contractuelle des tâches ne suffit pas à elle seule à déterminer la qualification juridique effective des acteurs.

En second lieu, la directive NIS 2 relative à la sécurité des réseaux et des systèmes d'information³⁹ illustre une évolution vers une régulation proactive de la cybersécurité. Elle impose aux entités concernées des obligations de gestion des risques, de notification des incidents et de mise en place de dispositifs de gouvernance adaptés. Cette logique préventive vise à réduire la survenance des incidents plutôt qu'à se limiter à leur sanction a posteriori.

En outre, certains systèmes juridiques européens, notamment en droit français et allemand, tendent à reconnaître des obligations de sécurité renforcées à la charge des prestataires numériques, en tenant compte des spécificités techniques des services fournis. Ces approches permettent d'adapter les catégories classiques du droit de la responsabilité aux réalités du numérique. À ce titre, des instruments plus récents s'inscrivent dans cette logique. Le règlement européen sur la cyber-résilience impose des exigences de sécurité dès la conception des produits comportant des éléments numériques⁴⁰. Le règlement DORA, propre au secteur financier, encadre quant à lui strictement le recours aux prestataires informatiques tiers, au premier rang desquels figurent les fournisseurs cloud, et va jusqu'à soumettre les prestataires critiques à une supervision directe⁴¹. Par ailleurs, des référentiels nationaux de qualification, tels que SecNumCloud en France⁴² ou le catalogue C5

39 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, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE), EP, CONSIL, 333 OJ L (2022), <http://data.europa.eu/eli/dir/2022/2555/oj>.

40 Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyber-résilience) (Texte présentant de l'intérêt pour l'EEE) (2024), <http://data.europa.eu/eli/reg/2024/2847/oj>.

41 Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 (Texte présentant de l'intérêt pour l'EEE), 333 OJ L (2022), <http://data.europa.eu/eli/reg/2022/2554/oj>.

42 Agence nationale de la sécurité des systèmes d'information (ANSSI), Référentiel d'exigences SecNumCloud, version en vigueur, rubrique « Prestataires de services d'informatique en nuage (SecNumCloud) ».

en Allemagne⁴³, mériteraient d'être étudiés pour affiner le référentiel marocain institué par le décret n° 2-24-921. Leur expérience pratique pourrait ainsi éclairer l'articulation nécessaire entre certification et responsabilité juridique du prestataire.

L'ensemble de ces éléments révèle une tendance commune : le passage d'une logique purement réparatrice à une logique intégrée, combinant prévention, responsabilisation et sanction. Cette évolution apparaît particulièrement pertinente dans le contexte du cloud computing, où la gestion des risques constitue un enjeu central.

Les recommandations 01/2020 du Comité européen de la protection des données (version finale du 18 juin 2021) offrent, quant à elles, un point de comparaison utile pour l'appréciation des mesures complémentaires en cas de transferts internationaux de données. Leur mobilisation dans le contexte marocain relève toutefois d'une proposition de convergence et non de l'affirmation de leur applicabilité directe aux contrats régis par le droit marocain.

Tableau 4 — Enseignements comparés et pistes de transposition prudente

Référence	Mécanisme pertinent	Piste pour le droit marocain
RGPD (art. 28, 32, 82)	Obligations du sous-traitant ; sécurité ; réparation	Clarifier rôles, devoirs documentés et recours
Directive NIS 2	Mesures de gestion du risque et notification	Renforcer prévention, supervision et notification dans les champs concernés
DORA (secteur financier)	Gouvernance du risque lié aux prestataires TIC	Exiger des garanties contractuelles dans les secteurs sensibles
SecNumCloud / BSI C5	Référentiels de confiance et d'audit	Affiner qualification, contrôles et production d'éléments vérifiables
CEPD, lignes directrices 07/2020 et recommandations 01/2020	Qualification des acteurs ; mesures complémentaires de transfert	Préciser responsabilités et critères de sécurité transfrontalière

Source : synthèse comparative des instruments cités ; les régimes européens ne sont pas présentés comme directement applicables au Maroc.

⁴³ Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloud Computing Compliance Controls Catalogue (C5), C5:2020.

2.2 – Propositions pour le droit marocain : vers un encadrement adapté de la responsabilité des prestataires cloud

À la lumière des insuffisances identifiées et des enseignements du droit comparé, plusieurs pistes de réforme peuvent être envisagées afin de renforcer l'effectivité du régime de responsabilité des prestataires de services cloud en droit marocain.

En premier lieu, il apparaît nécessaire de clarifier légalement la nature des obligations pesant sur les prestataires cloud, en consacrant explicitement la notion d'obligation de sécurité renforcée. Une telle clarification permettrait d'harmoniser l'interprétation des juridictions et de réduire l'incertitude juridique.

En deuxième lieu, un encadrement plus strict des clauses limitatives de responsabilité s'impose. Il conviendrait notamment de préciser les conditions dans lesquelles ces clauses peuvent être opposées au client, en particulier en cas de manquement aux obligations de sécurité. Une intervention législative pourrait viser à interdire ou à limiter ces clauses lorsqu'elles portent atteinte à l'obligation essentielle du prestataire.

En troisième lieu, la mise en place d'un régime probatoire adapté constitue une nécessité. À cet égard, l'instauration de mécanismes d'allègement de la charge de la preuve, voire de présomptions de responsabilité à la charge du prestataire en cas d'incident, permettrait de rééquilibrer les rapports entre les parties et d'assurer une meilleure protection des victimes. Un référentiel probatoire minimal pourrait utilement accompagner ce dispositif, imposant au prestataire la conservation et la remise au client des journaux d'événements, la traçabilité des accès et la préservation de la preuve numérique selon les standards internationaux.

En quatrième lieu, la question de l'extraterritorialité des services cloud doit être prise en compte. Il conviendrait de renforcer les règles relatives à la compétence juridictionnelle et au droit applicable, afin de garantir l'effectivité des recours contre les prestataires étrangers. Une coopération internationale accrue et l'intégration de clauses contractuelles spécifiques pourraient également être envisagées.

En cinquième lieu, d'autres mécanismes complémentaires soutiendraient l'effectivité du régime. Une obligation de notifier au client les incidents de sécurité dans un délai déterminé lui permettrait de réagir à temps et de limiter le préjudice. Le développement de l'assurance du risque cyber garantirait, quant à lui, la solvabilité de la réparation.

Enfin, une approche globale intégrant à la fois des mécanismes préventifs et répressifs devrait être privilégiée. Cette approche pourrait s'appuyer sur le renforcement des obligations de conformité,

la mise en place de mécanismes de certification des prestataires cloud et le développement de standards techniques reconnus.⁴⁴

Ainsi, l'adaptation du droit marocain aux enjeux du cloud computing ne suppose pas une rupture avec les principes existants, mais plutôt leur évolution afin de mieux prendre en compte les spécificités du numérique et de la cybersécurité.

Pour rendre ces propositions opératoires, une réforme graduée pourrait hiérarchiser les obligations en fonction de la criticité des données, de l'intensité du contrôle technique exercé par le fournisseur et de la capacité d'accès du client à la preuve. La conservation vérifiable des journaux, l'assistance à l'expertise contradictoire et la transparence des sous-traitances constitueraient des obligations documentaires particulièrement pertinentes pour relier conformité technique et réparation civile.

44 « Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services », <https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services>.

Conclusion

L'analyse de la responsabilité juridique des prestataires de services cloud face aux incidents de cybersécurité met en évidence la tension croissante entre les catégories classiques du droit des obligations et les réalités techniques des environnements numériques. Si le droit marocain offre des fondements juridiques permettant, en théorie, d'engager la responsabilité des prestataires, leur mise en œuvre se heurte à des limites structurelles liées à la complexité du cloud computing.

En effet, la qualification des obligations de cybersécurité, oscillant entre obligation de moyens et obligation renforcée, demeure incertaine et conditionne directement le régime probatoire applicable. À cela s'ajoutent des difficultés majeures en matière de preuve, résultant de l'asymétrie d'information entre prestataires et clients, ainsi que des obstacles liés à l'imputabilité des incidents dans un environnement caractérisé par la multiplicité des acteurs. Par ailleurs, le recours généralisé aux clauses limitatives de responsabilité contribue à restreindre l'effectivité de la réparation du préjudice, tandis que le modèle de responsabilité partagée, bien qu'opérationnel, introduit une ambiguïté persistante dans la répartition des obligations.

Ces constats révèlent les insuffisances du cadre juridique marocain, marqué par une fragmentation des sources et une adaptation encore partielle aux enjeux du numérique. La problématique posée appelle donc une réponse nuancée : le droit positif permet d'identifier certains manquements et d'engager la responsabilité du prestataire, mais il ne garantit pas encore une mise en œuvre suffisamment cohérente, prévisible et équilibrée face au risque cyber. L'hypothèse H1 est confirmée par l'absence d'un régime unifié propre à la responsabilité des prestataires cloud. L'hypothèse H2 est confirmée par les obstacles probatoires, causaux et transfrontaliers. L'hypothèse H3 est partiellement confirmée : le décret n° 2-24-921 et l'arrêté n° 3-17-25 renforcent la prévention et la qualification, tandis que les sanctions de la loi n° 09-08 existent, mais leur articulation avec la réparation civile et les clauses limitatives demeure incomplète. Enfin, l'hypothèse H4 est confirmée dans sa dimension prospective, les instruments européens et les référentiels français et allemand offrant des solutions transposables avec adaptation au contexte marocain.

Dans cette perspective, l'évolution du droit marocain apparaît nécessaire. Celle-ci devrait s'orienter vers une clarification normative des obligations des prestataires, un encadrement plus strict des mécanismes contractuels, notamment des clauses limitatives de responsabilité, ainsi qu'une adaptation du régime probatoire afin de mieux prendre en compte les spécificités techniques des incidents de cybersécurité. Par ailleurs, l'intégration des enseignements du droit comparé,

notamment européen, permettrait d'inscrire cette évolution dans une dynamique internationale, tout en tenant compte des particularités du contexte juridique national.

En définitive, la construction d'un régime de responsabilité adapté aux services cloud suppose une approche renouvelée du droit de la responsabilité, fondée sur un équilibre entre innovation technologique, sécurité juridique et protection effective des utilisateurs. Cette évolution constitue un enjeu majeur pour le développement d'un écosystème numérique sécurisé et juridiquement fiable au Maroc.

Bibliographie

1. Ouvrages et chapitres d'ouvrage

MATHER, T., KUMARASWAMY, S. et LATIF, S., Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.
<https://www.oreilly.com/library/view/cloud-security-and/9780596806453/>

DEHGANTANHA, A. et al. (dir.), Cyber Threat Intelligence, Springer, 2018.

MILLARD, C. (dir.), Cloud Computing Law, 2e éd., Oxford University Press, 2021.

PEARSON, S. et YEE, G. (dir.), Privacy and Security for Cloud Computing, Springer, 2013.

REED, C., Internet Law: Text and Materials, 2e éd., Cambridge University Press, 2004.

ROWLAND, D., KOHL, U. et CHARLESWORTH, A., Information Technology Law, 5e éd., Routledge, 2016.

2. Doctrine marocaine

BASSIME, L., « L'évolution du cadre de gouvernance et de contrôle du numérique au Maroc », in Mélanges en l'honneur du Pr Abdellatif Komat, Éditions EMI, 2025, p. 317-340.

ABOU EL JAOUAD, A., « La preuve numérique à l'épreuve de la cybercriminalité en droit marocain », Revue Droit & Société, n° 11, octobre 2023.

LAGTATI, K. et EL HAMEL, D., « La protection des données personnelles au Maroc à l'ère du numérique », Revue Internationale Burak des Études Juridiques et Économiques, vol. 1, n° 1, 2025, p. 236-248.

ROUINI, N. et EL AIDOUNI, A., « Analyse comparative de la réglementation sur la protection des données à caractère personnel entre le Maroc et l'Union européenne », Revue de Droit Civil, Économique et Comparé, vol. 4, n° 2, 2023.

3. Articles scientifiques et doctrine étrangère

SVANTESSON, D. et CLARKE, R., « Privacy and consumer risks in cloud computing », Computer Law & Security Review, vol. 26, n° 4, 2010, p. 391-397.
<https://doi.org/10.1016/j.clsr.2010.05.005>

HON, W. K., MILLARD, C. et WALDEN, I., « Who is responsible for "personal data" in cloud computing? The cloud of unknowing, Part 2 », International Data Privacy Law, vol. 2, n° 1, 2012, p. 3-18.

KHAN, S. et al., « A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned », ACM Transactions on Privacy and Security, vol. 26, n° 1, 2022.

SUBASHINI, S. et KAVITHA, V., « A Survey on Security Issues in Service Delivery Models of Cloud Computing », Journal of Network and Computer Applications, vol. 34, n° 1, 2011, p. 1-11.

TAKABI, H., JOSHI, J. et AHN, G.-J., « Security and Privacy Challenges in Cloud Computing Environments », IEEE Security & Privacy, vol. 8, n° 6, 2010, p. 24-31.

4. Textes juridiques marocains

Dahir formant Code des obligations et des contrats du 9 ramadan 1331 (12 août 1913), tel que modifié et complété.

Loi n° 53-05 relative à l'échange électronique de données juridiques, promulguée par le dahir n° 1-07-129 du 30 novembre 2007.

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

Loi n° 05-20 relative à la cybersécurité, promulguée par le dahir n° 1-20-69 du 25 juillet 2020.

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 ou de données sensibles, B.O. n° 7380 du 20 février 2025, p. 301.

Arrêté du Chef du gouvernement n° 3-17-25 du 7 safar 1447 (1er août 2025) fixant le référentiel des exigences de qualification des prestataires de services Cloud, B.O. n° 7432 du 21 août 2025, p. 2343.

5. Droit de l'Union européenne et droit américain

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD), Lignes directrices 07/2020 sur les notions de responsable du traitement et de sous-traitant dans le RGPD, version finale, 7 juillet 2021. https://www.edpb.europa.eu/documents/guideline/guidelines-072020-on-the-concepts-of-controller-and-processor-in-the-gdpr_en

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD), Recommandations 01/2020 sur les mesures qui complètent les outils de transfert, version finale, 18 juin 2021. https://www.edpb.europa.eu/documents/recommendation/recommendations-012020-on-measures-that-supplement-transfer-tools-to_en

Règlement (UE) 2016/679 du 27 avril 2016 (RGPD).

Directive (UE) 2022/2555 du 14 décembre 2022 (NIS 2).

Règlement (UE) 2024/2847 du 23 octobre 2024 sur la cyber-résilience (Cyber Resilience Act).

Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA).

Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 2018.

6. Conventions et jurisprudence

Convention du Conseil de l'Europe sur la cybercriminalité, Budapest, 23 novembre 2001.

Tribunal de commerce de Lille Métropole, 26 janvier 2023, contentieux consécutif à l'incendie du centre de données d'OVHcloud.

Microsoft Corp. v. United States, U.S. Court of Appeals for the Second Circuit, 14 juillet 2016.

In re Capital One Consumer Data Security Breach Litigation, MDL n° 1:19-md-2915 (E.D. Virginia).

In re Blackbaud, Inc. Customer Data Breach Litigation, MDL n° 2972 (D. South Carolina).

Office of the Comptroller of the Currency, Consent Order for the Assessment of a Civil Money Penalty, Capital One, AA-EC-2020-63, 2020.

7. Normes, référentiels et rapports institutionnels

JANSEN, W. et GRANCE, T., Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, décembre 2011. <https://doi.org/10.6028/NIST.SP.800-144>

NELSON, A., REKHI, S., SOUPPAYA, M. et SCARFONE, K., Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST SP 800-61 Rev. 3, avril 2025. <https://doi.org/10.6028/NIST.SP.800-61r3>

ANSSI, Référentiel d'exigences SecNumCloud, version en vigueur.

BSI, Cloud Computing Compliance Controls Catalogue (C5), C5:2020.

CNIL, Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services, 21 juin 2012.

ENISA, Cloud Computing: Benefits, Risks and Recommendations for Information Security, 2009, révisé en 2012.

ISO/IEC 27001 ; ISO/IEC 27017:2015 ; ISO/IEC 27018:2019 ; ISO/IEC 27037:2012.

MELL, P. et GRANCE, T., The NIST Definition of Cloud Computing, NIST SP 800-145, 2011. of Cloud Computing, NIST SP 800-145, 2011.