ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

La responsabilité des prestataires de cloud face aux violations de la propriété intellectuelle générées par l'intelligence artificielle : enjeux juridiques et défis probatoires

Liability of Cloud Service Providers for Intellectual Property Infringements Generated by Artificial Intelligence: Legal Issues and Evidentiary Challenges

Abir OMRI

Doctorante-chercheuse

Faculté des Sciences Juridiques et Politiques de Settat - Université Hassan 1er de Settat

abir.omri.doc@uhp.ac.ma

Pr. Soumaya AKKOUR

Professeure de l'Enseignement Supérieur - Faculté des Sciences Juridiques et Politiques de Settat - Université Hassan 1er de Settat

Résumé

Le développement simultané du cloud computing et de l'intelligence artificielle générative transforme profondément les conditions de création, de stockage, de reproduction et de diffusion des œuvres protégées. Les systèmes d'IA reposent fréquemment sur des infrastructures cloud pour l'entraînement des modèles, l'hébergement des jeux de données, l'exécution des traitements et la mise à disposition des contenus générés. Dans cet environnement, les atteintes à la propriété intellectuelle peuvent résulter de la reproduction non autorisée d'œuvres protégées, de la génération de contenus substantiellement similaires à des œuvres préexistantes ou encore de la diffusion automatisée de créations litigieuses à grande échelle. La question devient alors particulièrement délicate lorsque le prestataire de cloud n'est ni l'auteur direct de l'atteinte ni le titulaire du système d'IA, mais demeure l'acteur technique qui rend possible l'hébergement, le traitement et parfois l'optimisation du service numérique. Cette contribution analyse, dans une perspective théorique et juridique, les conditions dans lesquelles la responsabilité des prestataires de cloud peut être déterminée face aux violations de la propriété intellectuelle générées par l'IA. Elle met en évidence les difficultés de qualification juridique du rôle du prestataire, les limites des régimes classiques de responsabilité et les défis probatoires liés à l'identification de l'auteur, à la traçabilité des contenus et à l'imputabilité de la violation. L'article défend l'idée que la responsabilité du prestataire cloud doit être appréciée selon son degré de contrôle, sa connaissance effective de l'atteinte, sa capacité d'intervention et son niveau de coopération probatoire.

Mots-clés : Cloud computing ; intelligence artificielle ; propriété intellectuelle ; responsabilité ; preuve numérique ; imputabilité.

Abstract

The simultaneous development of cloud computing and generative artificial intelligence is reshaping the legal conditions under which protected works are created, stored, reproduced and disseminated. AI systems often rely on cloud infrastructures for model training, data hosting, computational processing and the distribution of generated outputs. In such

an environment, intellectual property infringements may arise from unauthorized reproduction of protected works, the generation of outputs substantially similar to pre-existing works or the automated dissemination of disputed content at scale. The liability of cloud service providers is particularly difficult to assess because they are not necessarily the direct infringers, yet they provide the technical infrastructure enabling storage, processing and distribution. This article adopts a theoretical and legal approach to examine how the liability of cloud providers may be determined in cases of AI-generated intellectual property infringements. It highlights the difficulty of legally qualifying the provider's role, the limits of traditional liability regimes and the evidentiary challenges relating to identification, traceability and imputability. The article argues that the liability of cloud providers should be assessed according to their degree of control, effective knowledge of the infringement, capacity to intervene and level of evidentiary cooperation.

Keywords: Cloud computing; artificial intelligence; intellectual property; liability; digital evidence; imputability.

Introduction

La transformation numérique de l'économie contemporaine est marquée par une convergence structurelle entre le cloud computing et l'intelligence artificielle. Le cloud n'est plus seulement un espace de stockage externalisé; il est devenu une infrastructure centrale de traitement, d'entraînement, de déploiement et de diffusion des systèmes intelligents. Les entreprises, les administrations, les plateformes numériques et les acteurs créatifs recourent désormais à des ressources cloud pour héberger des bases de données massives, exécuter des modèles d'intelligence artificielle, générer des images, des textes, des sons, des codes informatiques ou encore des contenus audiovisuels. Cette évolution modifie profondément la chaîne technique de production et de circulation des œuvres, mais elle déplace aussi les frontières classiques de la responsabilité juridique.[5120]

L'intelligence artificielle générative repose sur des processus techniques complexes. Elle peut être entraînée sur de très grands ensembles de données, parfois composés d'œuvres protégées par le droit d'auteur ou par des droits voisins. Elle peut ensuite produire des contenus susceptibles de reproduire des éléments substantiels d'œuvres antérieures, d'imiter un style, de générer des fragments textuels ou visuels similaires à des créations existantes, ou encore de faciliter la diffusion massive de contenus contrefaisants. Dès lors, la propriété intellectuelle se trouve confrontée à un double défi : protéger les titulaires de droits contre les usages non autorisés de leurs œuvres, tout en permettant l'innovation technologique et la circulation licite des connaissances. L'Organisation Mondiale de la Propriété Intellectuelle souligne d'ailleurs que l'essor de l'IA générative rend plus nécessaire une infrastructure du droit d'auteur capable d'assurer la transparence, le consentement et la compensation des créateurs.[5121]

Dans cette chaîne technologique, les prestataires de cloud occupent une position ambivalente. D'un côté, ils apparaissent comme des intermédiaires techniques fournissant des ressources de calcul, de stockage, de réseau et d'hébergement. Ils ne choisissent pas nécessairement les œuvres utilisées pour entraîner un système d'IA, ne rédigent pas directement les requêtes et ne décident pas toujours de diffuser les contenus générés. D'un autre côté, certains fournisseurs de cloud ne se limitent plus à une fonction passive : ils proposent des services intégrés d'intelligence artificielle, des interfaces de génération de

[5120] C. Millard (dir.), Cloud Computing Law, Oxford University Press, 2013; S. Russell et P. Norvig, Artificial Intelligence: A Modern Approach, 4e éd., Pearson, 2021.
[5121] Organisation Mondiale de la Propriété Intellectuelle (OMPI), Artificial Intelligence and Intellectual Property, WIPO, 2024.

contenus, des environnements d'apprentissage automatique, des outils d'analyse, des bibliothèques de modèles et des mécanismes d'automatisation. Cette évolution rend incertaine la frontière entre simple neutralité technique et participation active à un service susceptible de produire des atteintes à la propriété intellectuelle.

La question de la responsabilité devient alors centrale. Les régimes classiques de responsabilité civile exigent généralement l'identification d'une faute, d'un dommage et d'un lien de causalité. Les règles relatives à la contrefaçon supposent, quant à elles, de démontrer une reproduction, une représentation ou une exploitation non autorisée d'une œuvre protégée. Or, dans l'environnement cloud et IA, ces éléments deviennent difficiles à établir. Le dommage peut être diffus, l'auteur peut être multiple, le processus génératif peut être opaque et les preuves techniques peuvent être dispersées entre plusieurs acteurs et plusieurs juridictions. La difficulté n'est donc pas uniquement de qualifier l'atteinte; elle est aussi de déterminer à qui elle peut être juridiquement imputée.[5122]

La problématique retenue est la suivante : comment déterminer la responsabilité des prestataires de cloud en cas de violations de la propriété intellectuelle générées par l'intelligence artificielle, face aux difficultés de preuve et d'imputabilité? Cette problématique invite à dépasser une lecture purement technique du cloud pour analyser son rôle à travers le prisme de la responsabilité, du contrôle, de la connaissance effective de l'atteinte et de la coopération probatoire. Elle suppose également d'articuler le droit de la propriété intellectuelle, le droit des obligations, le droit du numérique, la cybersécurité, la preuve électronique et la régulation émergente de l'intelligence artificielle.

L'intérêt scientifique du sujet est important. Sur le plan théorique, il permet de renouveler la réflexion sur la responsabilité des intermédiaires numériques à l'ère de l'intelligence artificielle. Les catégories classiques d'hébergeur, de fournisseur technique, de sous-traitant numérique ou de prestataire d'infrastructure semblent insuffisantes lorsqu'un même acteur fournit à la fois l'environnement cloud, les outils d'IA, les services d'automatisation et parfois les mécanismes de distribution. Sur le plan pratique, l'étude concerne les titulaires de droits, les prestataires cloud, les développeurs d'IA, les utilisateurs professionnels et les juridictions appelées à apprécier des preuves numériques complexes. Sur le plan normatif, elle s'inscrit dans un contexte d'évolution du droit, marqué notamment par le Digital Services Act, l'AI Act européen, les exigences de traçabilité et les réflexions internationales sur l'IA et la propriété intellectuelle.[5123]

Le cadre d'analyse peut être inscrit dans une perspective marocaine ouverte au droit comparé. Au Maroc, la loi n° 2-00 relative aux droits d'auteur et droits voisins constitue le socle de protection des œuvres, tandis que le Code des obligations et contrats permet d'appréhender les mécanismes généraux de responsabilité. La loi n° 05-20 relative à la cybersécurité, le décret n° 2-24-921 relatif au recours aux prestataires de services cloud par certaines entités sensibles, ainsi que la loi n° 09-08 relative à la protection des données à caractère personnel, montrent que le cloud est désormais un objet de régulation juridique et non plus seulement une solution technique. Toutefois, ces textes ne règlent pas directement la responsabilité

[5122] A. Bensamoun et G. Loiseau, Droit du numérique : Contrats, innovation, données et gouvernance, Eyrolles, 2021; M. Vivant et J.-M. Bruguière, Droit d'auteur et droits voisins, Dalloz, 2023.

[5123] Union européenne, Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques (Digital Services Act), Journal officiel de l'Union européenne, 2022; Union européenne, Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act), Journal officiel de l'Union européenne, 2024.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

des prestataires cloud face aux atteintes à la propriété intellectuelle générées par l'IA, ce qui justifie une approche doctrinale et prospective.[5124]

Sur le plan méthodologique, cette étude adopte une approche théorique, juridique et analytique. Elle repose sur l'examen des textes relatifs à la propriété intellectuelle, à la responsabilité civile, au cloud computing, à la cybersécurité et à l'intelligence artificielle. Elle mobilise également une approche comparative en s'appuyant sur les orientations européennes et internationales, notamment en matière de responsabilité des intermédiaires, de transparence des systèmes d'IA et de protection des titulaires de droits. Cette méthode permet d'identifier les limites des régimes actuels, de comprendre les difficultés probatoires et de proposer des pistes de clarification du régime de responsabilité applicable aux prestataires cloud.

L'hypothèse défendue est que la responsabilité des prestataires de cloud ne peut être déterminée de manière uniforme. Elle doit dépendre du rôle concret joué par le prestataire dans la chaîne de production, d'hébergement ou de diffusion du contenu litigieux. Un prestataire purement passif, dépourvu de connaissance effective et de capacité raisonnable d'intervention, ne saurait être assimilé à l'auteur direct de la violation. En revanche, un prestataire qui propose des outils d'IA intégrés, optimise la génération de contenus, contrôle les conditions de diffusion ou refuse d'agir après notification d'une atteinte peut voir sa responsabilité renforcée. Ainsi, la solution réside moins dans une responsabilité automatique que dans une responsabilité graduée, fondée sur le contrôle, la connaissance, la diligence et la traçabilité.

Pour répondre à cette problématique, l'étude sera structurée autour de deux axes. La première partie analysera la difficile détermination de la responsabilité des prestataires de cloud face aux violations de la propriété intellectuelle générées par l'IA. Elle examinera la qualification juridique du rôle du prestataire et les limites des régimes classiques de responsabilité. La seconde partie sera consacrée aux défis probatoires et aux perspectives d'évolution du régime de responsabilité, en mettant l'accent sur l'identification de l'auteur, la preuve numérique, la traçabilité et la nécessité d'un encadrement juridique plus adapté.

1. La détermination de la responsabilité des prestataires de cloud face aux violations de la propriété intellectuelle générées par l'IA

La détermination de la responsabilité des prestataires de cloud suppose d'abord de clarifier leur place dans l'écosystème technique de l'intelligence artificielle. En matière numérique, la responsabilité ne peut être appréciée sans une analyse fonctionnelle du rôle joué par chaque acteur. Le prestataire cloud peut intervenir comme fournisseur d'infrastructure, hébergeur de données, opérateur de services applicatifs, distributeur d'outils d'IA ou partenaire contractuel d'un développeur. Chacune de ces fonctions correspond à un niveau différent de contrôle et donc à une intensité variable de responsabilité. La difficulté vient du fait que les services cloud contemporains combinent souvent plusieurs niveaux : infrastructure, plateforme, logiciel, modèle d'IA et outils d'intégration.

Le droit de la propriété intellectuelle est traditionnellement construit autour d'actes identifiables : reproduction, représentation, adaptation, distribution, communication au public ou mise à disposition. Dans un environnement cloud,

[5124] Loi n° 2-00 relative aux droits d'auteur et droits voisins, promulguée par le Dahir n° 1-00-20 du 15 février 2000, telle que modifiée et complétée; Loi n° 05-20 relative à la cybersécurité, promulguée par le Dahir n° 1-20-69 du 25 juillet 2020; 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; Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services cloud par les entités et infrastructures concernées.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

ces actes peuvent être fragmentés. Une œuvre peut être copiée dans un jeu de données, stockée sur un serveur, transformée par un modèle d'IA, intégrée dans un résultat généré puis diffusée via une interface numérique. Chaque étape peut être opérée par un acteur différent. Le prestataire cloud se situe souvent en arrière-plan technique, mais il conserve parfois la maîtrise des environnements de calcul et des traces nécessaires à la preuve. Cette position intermédiaire explique l'incertitude de son régime de responsabilité.[5125]

1.1. La qualification juridique complexe du rôle du prestataire de cloud

Le premier enjeu consiste à qualifier juridiquement le prestataire de cloud. Cette qualification détermine le régime applicable : responsabilité directe, responsabilité indirecte, responsabilité contractuelle, responsabilité délictuelle ou régime atténué applicable à certains intermédiaires numériques. Or, le cloud computing ne correspond pas à une catégorie juridique unique. Il désigne un ensemble de services techniques permettant l'accès à des ressources informatiques mutualisées, évolutives et disponibles à distance. Selon la nature du service, le prestataire peut être plus ou moins proche du contenu traité et plus ou moins capable d'intervenir sur les données hébergées.[5126]

La doctrine distingue généralement plusieurs modèles : Infrastructure as a Service, Platform as a Service et Software as a Service. Dans le premier modèle, le prestataire fournit principalement des ressources de calcul, de stockage et de réseau. Dans le deuxième, il met à disposition un environnement technique permettant le développement et l'exécution d'applications. Dans le troisième, il propose directement un service applicatif utilisable par le client final. Cette distinction, issue de la technique, a des conséquences juridiques importantes. Plus le prestataire se rapproche de la couche applicative et du contrôle fonctionnel du service, plus il devient difficile de le considérer comme un simple intermédiaire passif.[5127]

En matière d'intelligence artificielle, cette gradation est encore plus importante. Un fournisseur qui se limite à louer des serveurs pour l'entraînement d'un modèle ne joue pas le même rôle qu'un fournisseur qui propose un service complet de génération d'images, de textes ou de musiques. Dans le premier cas, il fournit une infrastructure; dans le second, il participe à l'organisation du service génératif. La qualification doit donc être concrète et non abstraite. Elle doit prendre en considération le degré d'intervention du prestataire dans la conception du service, l'accès aux données, la configuration du modèle, la surveillance des usages, la modération des contenus et la capacité de blocage ou de retrait.

Le Digital Services Act européen illustre cette logique en différenciant les obligations selon le rôle, la taille et l'impact du service dans l'écosystème numérique. Même si ce règlement ne vise pas spécifiquement tous les services cloud de manière uniforme, il consacre une méthode utile : les obligations doivent être proportionnées au rôle du prestataire et à sa capacité d'action. Cette approche permet d'éviter deux excès. Le premier serait d'exonérer systématiquement les prestataires cloud au motif qu'ils sont techniques. Le second serait de leur imposer une responsabilité générale pour tous les contenus générés par les utilisateurs ou par des systèmes d'IA hébergés sur leurs infrastructures.[5128]

La qualification du prestataire de cloud doit aussi être distinguée de celle du fournisseur du modèle d'IA. Dans certains cas, ces deux fonctions sont exercées par le même groupe ou par des entités contractuellement liées. Dans d'autres cas, le cloud

[5125] Loi n° 2-00 relative aux droits d'auteur et droits voisins, précitée; World Intellectual Property Organization, WIPO Copyright Treaty, WIPO, 1996; World Trade Organization, Agreement on Trade-Related Aspects of Intellectual Property Rights, WTO, 1994; P. Sirinelli, Propriété littéraire et artistique, Dalloz, 2022.
[5126] C. Millard (dir.), Cloud Computing Law, Oxford University Press, 2013.
[5127] C. Millard (dir.), op. cit., 2013.
[5128] Union européenne, Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques (Digital Services Act), Journal officiel de l'Union européenne, 2022.

est fourni par un acteur indépendant tandis que le modèle appartient à une autre entreprise. La confusion entre ces rôles peut conduire à une mauvaise imputation de la responsabilité. Le juge ou l'autorité compétente doit donc analyser la chaîne contractuelle et technique : qui a entraîné le modèle? qui a choisi les données? qui a formulé la requête? qui a généré le contenu? qui l'a stocké? qui l'a rendu accessible? qui pouvait empêcher ou retirer le contenu litigieux?

1.1.1. Le prestataire de cloud comme intermédiaire technique

Dans son acception la plus classique, le prestataire de cloud apparaît comme un intermédiaire technique. Il fournit des ressources informatiques nécessaires au fonctionnement d'un service numérique, sans intervenir directement dans le choix des contenus. Cette fonction se rapproche de celle de l'hébergeur ou du fournisseur d'infrastructure. Le prestataire ne crée pas l'œuvre litigieuse, ne détermine pas nécessairement les finalités du traitement et n'a pas toujours connaissance des données hébergées. Cette neutralité technique justifie l'existence de régimes de responsabilité atténuée dans plusieurs systèmes juridiques, notamment lorsque l'intermédiaire n'a pas connaissance effective du caractère illicite du contenu et agit rapidement après notification.[5129]

Toutefois, la neutralité ne doit pas être présumée de manière absolue. Le cloud computing repose sur des contrats, des politiques d'usage acceptable, des mécanismes de sécurité, des outils de surveillance et des capacités d'administration. Le prestataire dispose souvent de moyens techniques lui permettant de suspendre un compte, de bloquer un service, de conserver des journaux d'activité ou de coopérer avec une autorité judiciaire. Même s'il n'a pas vocation à surveiller tous les contenus de manière générale, il peut devenir juridiquement responsable lorsqu'il est informé d'une atteinte précise et qu'il ne prend aucune mesure raisonnable. La connaissance effective constitue alors un critère central de passage d'une neutralité technique à une responsabilité potentielle.

Dans le domaine de la propriété intellectuelle, cette connaissance peut résulter d'une notification du titulaire de droits, d'une décision judiciaire, d'un signalement circonstancié ou d'un mécanisme interne de détection. La difficulté réside dans la qualité de l'information fournie. Une simple allégation générale d'utilisation d'œuvres protégées ne suffit pas toujours à déclencher une obligation d'intervention, surtout lorsque l'atteinte suppose une analyse juridique complexe. En revanche, une notification précise identifiant l'œuvre protégée, le contenu litigieux, l'URL ou l'environnement cloud concerné, ainsi que les éléments de similarité, peut renforcer l'obligation de diligence du prestataire. La responsabilité devient alors liée à la réaction du prestataire après notification.

Cette approche est cohérente avec l'idée selon laquelle le prestataire cloud ne doit pas être transformé en juge permanent de la licéité des contenus. Une obligation générale de surveillance serait techniquement lourde, économiquement coûteuse et juridiquement problématique au regard des libertés numériques. Mais l'absence totale d'obligation de coopération priverait les titulaires de droits de toute efficacité dans l'environnement cloud. La solution doit donc être intermédiaire : pas de responsabilité automatique du prestataire pour toute violation générée par l'IA, mais une responsabilité possible en cas de connaissance effective, d'inaction fautive ou de contribution technique active à la persistance de l'atteinte.

1.1.2. Le prestataire de cloud comme acteur actif dans les services d'IA

La situation change lorsque le prestataire cloud ne se limite plus à fournir une infrastructure. Certains acteurs proposent désormais des services intégrés d'IA, des modèles pré-entraînés, des interfaces de génération, des outils de traitement de données et des environnements automatisés de déploiement. Dans ce cas, le prestataire n'est plus seulement le propriétaire

[5129] Union européenne, Règlement (UE) 2022/2065 (Digital Services Act), précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

des serveurs; il devient l'architecte d'un écosystème technologique permettant la production de contenus. Cette évolution justifie une analyse plus exigeante de sa responsabilité, car le prestataire peut influencer les conditions de génération, les garde-fous techniques, les filtres de contenu, les politiques d'utilisation et les modalités de conservation des preuves.[5130]

L'AI Act européen adopte une logique de responsabilité distribuée entre les différents opérateurs de la chaîne de valeur de l'intelligence artificielle, notamment les fournisseurs et les déployeurs de systèmes d'IA. Même si le prestataire cloud n'est pas toujours assimilable à un fournisseur d'IA au sens strict, cette approche montre que la responsabilité doit suivre le contrôle effectif. Celui qui conçoit, met sur le marché, déploie ou influence substantiellement le fonctionnement d'un système doit assumer des obligations proportionnées à son rôle. Appliquée au cloud, cette logique conduit à examiner si le prestataire fournit uniquement une capacité technique ou s'il participe à la mise en œuvre opérationnelle du système génératif.[5131]

Lorsque le prestataire propose lui-même des outils de génération de contenus, il doit anticiper les risques de violation de la propriété intellectuelle. Cette anticipation peut se traduire par des clauses contractuelles interdisant l'usage illicite d'œuvres protégées, des mécanismes de filtrage raisonnables, des dispositifs de traçabilité, des procédures de notification et de retrait, ainsi que des obligations de coopération avec les titulaires de droits. Le défaut de mise en place de ces mesures, surtout lorsque le service est conçu pour générer massivement des contenus créatifs, peut être analysé comme un manquement à une obligation de diligence.[5132]

La responsabilité du prestataire actif ne signifie pas nécessairement qu'il devient responsable de tous les résultats générés par les utilisateurs. Elle signifie plutôt que son comportement doit être apprécié à partir de son pouvoir d'organisation. S'il crée un environnement qui facilite les atteintes répétées, s'il ignore des signalements précis, s'il ne conserve aucune trace exploitable ou s'il organise contractuellement son irresponsabilité totale, son rôle ne peut plus être réduit à une pure neutralité. Le critère pertinent devient alors celui de la maîtrise raisonnable du risque : plus le prestataire dispose de moyens pour prévenir, limiter ou documenter les violations, plus son obligation de diligence doit être élevée.

1.2. Les limites des régimes classiques de responsabilité face aux atteintes générées par l'IA

Les régimes classiques de responsabilité ont été conçus pour des situations dans lesquelles l'auteur du dommage, l'acte illicite et le lien de causalité peuvent être identifiés avec une relative précision. L'intelligence artificielle générative et le cloud computing compliquent ce schéma. La violation peut résulter d'une combinaison entre les données d'entraînement, les paramètres du modèle, la requête formulée par l'utilisateur, l'algorithme de génération, les filtres appliqués, l'hébergement cloud et la diffusion du résultat. Cette fragmentation rend difficile la mise en œuvre des catégories traditionnelles de faute, de causalité et d'imputabilité.[5133]

[5130] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), U.S. Department of Commerce, 2023; S. Russell et P. Norvig, Artificial Intelligence: A Modern Approach, 4e éd., Pearson, 2021.

[5131] Union européenne, Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act), Journal officiel de l'Union européenne, 2024.

[5132] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023; A. Bensamoun et G. Loiseau, Droit du numérique : Contrats, innovation, données et gouvernance, Eyrolles, 2021.

[5133] R. Abbott, The Reasonable Robot: Artificial Intelligence and the Law, Cambridge University Press, 2020; K. Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence, Yale University Press, 2021.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

La propriété intellectuelle repose également sur des notions qui deviennent délicates dans l'environnement génératif. Il faut déterminer si le résultat produit par l'IA reproduit une œuvre protégée, s'il constitue une simple inspiration, s'il reprend des éléments originaux, s'il relève d'une exception ou s'il s'agit d'une création autonome. Ces questions sont déjà complexes entre auteurs humains; elles le deviennent davantage lorsque le contenu est produit par un système probabiliste. Le prestataire cloud, situé en arrière-plan technique, n'est pas toujours en mesure d'apprécier juridiquement la similarité substantielle entre une œuvre protégée et une sortie générée par l'IA.[5134]

1.2.1. L'insuffisance des règles classiques de la responsabilité civile

En droit civil, la responsabilité suppose généralement la réunion de trois éléments : un fait générateur, un dommage et un lien de causalité. Dans l'hypothèse d'une violation de propriété intellectuelle générée par l'IA, ces éléments existent en apparence, mais leur démonstration est particulièrement difficile. Le dommage peut consister dans une perte économique, une atteinte au monopole d'exploitation, une dilution de la valeur de l'œuvre, une concurrence déloyale ou une atteinte morale. Le fait générateur peut être l'utilisation non autorisée d'une œuvre, la génération d'un contenu similaire ou la mise à disposition d'un fichier illicite. Le lien causal, en revanche, est souvent le plus difficile à établir.[5135]

Le prestataire cloud peut soutenir que le dommage résulte du comportement de l'utilisateur, du fournisseur du modèle d'IA ou du développeur qui a entraîné l'algorithme. Le titulaire de droits peut répondre que le prestataire a permis matériellement l'hébergement, le traitement ou la diffusion du contenu. Cette opposition révèle l'insuffisance d'une causalité purement matérielle. Si toute infrastructure technique devient causalement impliquée dans un dommage numérique, la responsabilité risque de s'étendre indéfiniment. Il faut donc distinguer la causalité matérielle, qui peut être très large, de l'imputabilité juridique, qui suppose un lien plus qualifié entre le comportement du prestataire et l'atteinte.

La faute du prestataire peut prendre plusieurs formes : défaut de réaction après notification, absence de conservation des preuves, violation d'une obligation contractuelle de sécurité, non-respect d'une décision judiciaire, assistance technique consciente à une activité illicite ou refus de coopérer avec l'autorité compétente. En revanche, le seul fait de fournir une infrastructure cloud utilisée par un tiers pour commettre une violation ne devrait pas suffire à engager automatiquement la responsabilité du prestataire. Une telle automaticité ferait peser sur les acteurs techniques une charge excessive et pourrait freiner l'innovation numérique.

La responsabilité contractuelle joue également un rôle important. Les contrats de cloud contiennent généralement des clauses relatives aux usages interdits, à la propriété des contenus, à la limitation de responsabilité, à la sécurité, à la résiliation, aux audits et à la coopération. Ces clauses organisent les relations entre le prestataire et son client, mais elles ne suffisent pas toujours à protéger les titulaires de droits tiers. L'enjeu est donc d'articuler le contrat et la responsabilité extracontractuelle. Le prestataire peut limiter sa responsabilité contractuelle vis-à-vis de son client, mais il ne devrait pas pouvoir se soustraire à toute obligation légale de coopération lorsqu'une atteinte précise aux droits d'autrui est démontrée.[5136]

Le droit marocain, à travers le Code des obligations et contrats, offre des catégories générales de responsabilité qui peuvent être mobilisées. Toutefois, ces catégories restent générales et ne répondent pas spécifiquement aux questions posées par le

[5134] J. C. Ginsburg et L. A. Budiardjo, « Authors and Machines », Berkeley Technology Law Journal, vol. 34, n° 2, 2019, p. 343-448; R. Abbott, op. cit., 2020.
[5135] A. Bensamoun et G. Loiseau, op. cit., 2021.
[5136] C. Millard (dir.), op. cit., 2013; A. Bensamoun et G. Loiseau, op. cit., 2021.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

cloud et l'IA. La loi n° 05-20 relative à la cybersécurité et le décret n° 2-24-921 sur le recours aux prestataires cloud par certaines entités sensibles montrent une tendance vers la responsabilisation des prestataires technologiques, mais principalement sous l'angle de la sécurité et de la souveraineté numérique. La propriété intellectuelle générée ou violée par l'IA nécessite encore une construction doctrinale et jurisprudentielle plus précise.[5137]

1.2.2. Les difficultés d'application du droit de la propriété intellectuelle aux contenus générés par l'IA

Le droit d'auteur protège les œuvres originales, c'est-à-dire les créations de forme portant l'empreinte de la personnalité de leur auteur. L'intelligence artificielle générative perturbe cette conception car elle produit des contenus sans intention créatrice humaine directe au moment de la génération. La première difficulté consiste à savoir si le contenu généré par l'IA peut lui-même être protégé. La seconde, plus importante pour le présent sujet, consiste à déterminer si ce contenu porte atteinte à des œuvres préexistantes. En pratique, une sortie d'IA peut reproduire des passages, des structures, des images, des mélodies ou des éléments visuels proches d'une œuvre protégée, sans que l'utilisateur ait nécessairement voulu copier cette œuvre.[5138]

La violation peut intervenir à deux niveaux. Le premier niveau est celui de l'entraînement du modèle. Si des œuvres protégées sont intégrées dans les jeux de données sans autorisation, la question de la reproduction technique et de l'éventuelle exception de fouille de textes et de données se pose. Le second niveau est celui de la sortie générée. Même si l'entraînement était licite, le résultat produit peut être contrefaisant s'il reprend des éléments originaux d'une œuvre protégée. Le prestataire cloud peut être impliqué à l'un ou l'autre niveau : il peut héberger les données d'entraînement, fournir la puissance de calcul, stocker le modèle, exécuter les requêtes ou diffuser les sorties.[5139]

Le droit européen a commencé à répondre à certains aspects de cette problématique. La directive 2019/790 sur le droit d'auteur dans le marché unique numérique encadre notamment certaines pratiques de fouille de textes et de données, tandis que l'AI Act impose aux fournisseurs de modèles d'IA à usage général certaines obligations de transparence, notamment en lien avec les contenus utilisés pour l'entraînement. Ces instruments ne règlent toutefois pas entièrement la responsabilité des prestataires cloud. Ils confirment surtout que la transparence des données, la documentation des modèles et la traçabilité des opérations deviennent essentielles pour permettre l'exercice effectif des droits de propriété intellectuelle.[5140]

Dans le contexte marocain, la loi n° 2-00 relative aux droits d'auteur et droits voisins protège les œuvres et organise les droits patrimoniaux et moraux. Cependant, elle n'a pas été conçue pour les hypothèses spécifiques de génération automatisée, d'entraînement massif de modèles ou d'hébergement cloud de systèmes d'IA. Cette situation ne signifie pas que les titulaires de droits sont dépourvus de protection, mais que l'application des règles existantes exige un effort d'interprétation. Il faut notamment déterminer si les actes techniques réalisés dans le cloud constituent des reproductions

[5137] Loi n° 05-20 relative à la cybersécurité, précitée; Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services cloud, précité.
[5138] P. Sirinelli, Propriété littéraire et artistique, Dalloz, 2022; J. C. Ginsburg et L. A. Budiardjo, art. préc., 2019; M. Vivant et J.-M. Bruguière, Droit d'auteur et droits voisins, Dalloz, 2023.
[5139] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique, Journal officiel de l'Union européenne.
[5140] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique, Journal officiel de l'Union européenne; Union européenne, Règlement (UE) 2024/1689 (AI Act), précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

juridiquement pertinentes, si la mise à disposition d'une sortie générée équivaut à une communication au public et si le prestataire cloud peut être qualifié de participant à l'exploitation illicite.[5141]

La difficulté est renforcée par la question de l'originalité et de la similarité substantielle. Une IA peut produire un résultat qui ressemble fortement à une œuvre sans en reproduire exactement les éléments. La preuve de la contrefaçon exige alors une comparaison fine entre l'œuvre protégée et le contenu généré. Cette comparaison peut nécessiter une expertise technique et artistique. Le prestataire cloud, de son côté, peut ne pas être en mesure d'évaluer la contrefaçon sans une décision judiciaire ou une notification très circonstanciée. Cette réalité plaide pour un régime de responsabilité graduée : l'obligation du prestataire ne doit pas être de trancher toutes les questions de propriété intellectuelle, mais de préserver les preuves, coopérer et agir en présence d'une atteinte manifestement identifiée.[5142]

La question des droits voisins et des attributs de la personnalité mérite également attention. Les contenus générés par IA peuvent imiter une voix, une image, une prestation artistique ou un style associé à un créateur. Ces atteintes ne relèvent pas toujours strictement du droit d'auteur; elles peuvent mobiliser les droits voisins, le droit à l'image, la concurrence déloyale ou la responsabilité civile. Le prestataire cloud peut être sollicité pour retirer des fichiers, identifier un compte ou conserver les traces de génération. Cette pluralité de fondements juridiques renforce encore la nécessité de mécanismes probatoires fiables.[5143]

2. Les défis probatoires et les perspectives d'évolution du régime de responsabilité des prestataires de cloud

La seconde dimension du sujet concerne la preuve. En droit numérique, l'effectivité de la responsabilité dépend largement de la capacité à établir les faits. Une règle de responsabilité peut être théoriquement satisfaisante mais pratiquement inefficace si le titulaire des droits ne peut pas identifier l'auteur de la violation, localiser le contenu litigieux, prouver la reproduction, accéder aux journaux d'activité ou démontrer le rôle du prestataire cloud. La preuve devient donc le cœur opérationnel de la responsabilité.

Les atteintes à la propriété intellectuelle générées par l'IA sont particulièrement difficiles à prouver en raison de l'opacité des modèles, de la volatilité des données, de la dispersion internationale des serveurs et de la multiplicité des intervenants. Les preuves peuvent exister sous forme de logs, métadonnées, historiques de requêtes, empreintes numériques, versions de modèles, fichiers temporaires ou traces d'accès. Mais ces éléments sont souvent détenus par les prestataires techniques eux-mêmes. Le titulaire de droits se trouve ainsi dans une situation d'asymétrie informationnelle : il subit ou constate l'atteinte, mais il ne possède pas les informations nécessaires pour l'imputer.[5144]

2.1. Les défis probatoires liés aux violations de la propriété intellectuelle générées par l'IA

Les défis probatoires se manifestent à plusieurs niveaux. Il faut d'abord prouver l'existence d'une œuvre protégée et l'atteinte portée à cette œuvre. Il faut ensuite démontrer que le contenu litigieux a été généré, stocké ou diffusé à travers un service déterminé. Il faut enfin établir le lien entre l'utilisateur, le système d'IA, le prestataire cloud et la violation. Cette

[5141] Loi n° 2-00 relative aux droits d'auteur et droits voisins, précitée.
[5142] S. Dusollier, Droit d'auteur et protection des œuvres dans l'univers numérique, Larcier, 2020; M. Vivant et J.-M. Bruguière, op. cit., 2023; T. Aplin et L. Bently, Global Mandatory Fair Use: The Nature and Scope of the Right to Quote Copyright Works, Cambridge University Press, 2020.
[5143] Loi n° 2-00 relative aux droits d'auteur et droits voisins, précitée; P. Sirinelli, op. cit., 2022.
[5144] National Institute of Standards and Technology, AI RMF 1.0, précité; K. Crawford, op. cit., 2021.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

dernière étape est la plus sensible, car elle suppose de transformer des traces techniques en preuves juridiquement exploitables.

La preuve numérique n'est pas seulement une question de collecte. Elle exige la conservation de l'intégrité des éléments, la traçabilité de leur origine, la datation, l'identification des accès, la protection contre l'altération et la possibilité de contradiction. Dans un contentieux relatif à l'IA, les preuves peuvent être contestées au motif qu'elles sont incomplètes, modifiables, non horodatées ou issues d'un système opaque. La responsabilité des prestataires cloud dépend donc aussi de leur capacité à organiser une preuve fiable, documentée et opposable.[5145]

2.1.1. La difficulté d'identifier l'auteur de la violation

L'identification de l'auteur est l'une des difficultés majeures. Dans un schéma classique de contrefaçon, l'auteur de l'acte illicite est souvent celui qui reproduit, vend, diffuse ou communique l'œuvre sans autorisation. Dans l'environnement IA-cloud, plusieurs acteurs peuvent intervenir successivement ou simultanément. L'utilisateur formule une requête, le modèle génère un résultat, le fournisseur du modèle détermine l'architecture algorithmique, le prestataire cloud fournit l'infrastructure, et une plateforme peut ensuite diffuser le contenu. L'auteur juridique de la violation ne se confond donc pas nécessairement avec l'acteur technique qui a rendu l'acte possible.

L'IA introduit également un effet d'autonomie apparente. Le contenu litigieux semble être produit par la machine, mais la machine n'est pas un sujet de droit responsable. L'imputabilité doit donc être recherchée du côté des personnes physiques ou morales qui conçoivent, exploitent, utilisent ou contrôlent le système. Cette recherche peut conduire vers l'utilisateur lorsqu'il a volontairement demandé la reproduction d'une œuvre protégée, vers le fournisseur du modèle lorsqu'il a organisé un système générant régulièrement des contenus contrefaisants, ou vers le prestataire cloud lorsqu'il a participé activement au service ou a refusé d'agir après connaissance de l'atteinte.[5146]

La difficulté tient au fait que les utilisateurs peuvent être anonymes, utiliser des comptes temporaires, accéder au service depuis plusieurs pays ou effacer les contenus litigieux. Les systèmes cloud peuvent répartir les données entre plusieurs centres de données et plusieurs sous-traitants. Les logs peuvent être conservés pour une durée limitée. Certaines requêtes peuvent ne pas être stockées pour des raisons de confidentialité ou de protection des données personnelles. La preuve de l'identité de l'auteur suppose donc une politique de conservation équilibrée, permettant à la fois la protection de la vie privée et la défense des droits de propriété intellectuelle.[5147]

L'imputabilité ne doit pas être confondue avec la simple identification technique. Connaître l'adresse IP ou le compte utilisateur ne suffit pas toujours à établir la responsabilité juridique. Il faut encore démontrer que la personne identifiée a effectivement généré ou diffusé le contenu litigieux, qu'elle avait la maîtrise de l'acte et que cet acte constitue une violation. Dans certains cas, l'utilisateur peut soutenir qu'il ignorait l'origine protégée du contenu généré. Dans d'autres, le prestataire peut soutenir qu'il n'avait aucune connaissance de la violation. Le débat probatoire devient alors un débat sur la connaissance, la prévisibilité et la diligence.

[5145] A. Bensamoun et G. Loiseau, op. cit., 2021; National Institute of Standards and Technology, AI RMF 1.0, précité.
[5146] R. Abbott, op. cit., 2020.
[5147] Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, précitée; Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP), Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, 2023.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

L'opacité des systèmes d'IA renforce cette difficulté. Les modèles génératifs ne produisent pas toujours des résultats identiques à partir d'une même requête. Leur fonctionnement probabiliste peut rendre difficile la reproduction exacte du processus ayant conduit au contenu litigieux. Pour établir l'imputabilité, il peut être nécessaire de conserver la version du modèle, la requête, les paramètres, le contexte, les filtres appliqués et l'horodatage de la génération. Sans ces éléments, il devient difficile de savoir si le contenu litigieux résulte d'un usage intentionnel, d'un défaut du modèle, d'un entraînement problématique ou d'une diffusion ultérieure.[5148]

2.1.2. La complexité de la preuve numérique dans l'environnement cloud

La preuve numérique dans l'environnement cloud repose principalement sur des traces techniques. Les logs d'accès, les métadonnées, les empreintes numériques, les historiques de requêtes, les journaux d'administration et les rapports d'incident peuvent permettre de reconstituer la chaîne des événements. Toutefois, ces éléments ne sont pas toujours accessibles au titulaire de droits. Ils sont souvent détenus par le prestataire cloud, par le fournisseur du modèle ou par le client professionnel. Cette asymétrie justifie l'importance d'obligations de conservation et de coopération probatoire.[5149]

Les logs ont une valeur particulière. Ils peuvent indiquer la date de création d'un fichier, l'identité d'un compte, l'adresse de connexion, le service utilisé, les actions réalisées, les modifications opérées et les accès successifs. Mais leur force probante dépend de leur fiabilité. Des logs incomplets, non horodatés, non sécurisés ou facilement modifiables peuvent être contestés. Il est donc nécessaire que les prestataires cloud mettent en place des mécanismes d'intégrité, d'horodatage, de contrôle d'accès et de conservation proportionnée. La preuve ne doit pas être improvisée après le litige; elle doit être intégrée dès la conception du service.

La conservation des preuves soulève cependant des tensions juridiques. D'un côté, les titulaires de droits ont besoin d'éléments techniques pour établir la violation. De l'autre, la conservation excessive de données peut porter atteinte à la vie privée, au secret des affaires ou à la sécurité des systèmes. La loi n° 09-08 au Maroc, comme le RGPD dans l'Union européenne, impose des principes de finalité, de proportionnalité et de limitation de conservation. Le défi consiste donc à définir des durées et des catégories de traces adaptées au risque, sans instaurer une surveillance générale des utilisateurs.[5150]

La preuve est également compliquée par la localisation des données. Les environnements cloud peuvent être transfrontaliers. Les données peuvent être hébergées dans un pays, traitées dans un autre et consultées depuis un troisième. Cette dispersion pose des questions de compétence juridictionnelle, de loi applicable, de transfert de données et d'exécution des décisions judiciaires. Le décret marocain n° 2-24-921 relatif au recours aux prestataires de services cloud par certaines entités et infrastructures sensibles montre l'importance croissante de la localisation, de la qualification des prestataires et de la maîtrise des données sensibles. Même si ce décret vise prioritairement la cybersécurité et la souveraineté numérique, sa logique peut inspirer la réflexion sur la preuve et la coopération des prestataires cloud.[5151]

Le recours à l'expertise technique devient souvent indispensable. Un expert peut comparer les œuvres, analyser les métadonnées, vérifier les logs, examiner les paramètres d'un modèle, apprécier la vraisemblance d'une reproduction ou

[5148] S. Russell et P. Norvig, op. cit., 2021; National Institute of Standards and Technology, AI RMF 1.0, précité.
[5149] C. Millard (dir.), op. cit., 2013.
[5150] Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, précitée; CNDP, op. cit., 2023.
[5151] Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services cloud, précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

reconstituer la trajectoire d'un contenu. Toutefois, l'expertise se heurte elle-même à l'opacité des systèmes et au secret des affaires. Les fournisseurs d'IA peuvent refuser de divulguer certains éléments relatifs aux données d'entraînement ou à l'architecture des modèles. Les prestataires cloud peuvent invoquer la confidentialité des autres clients ou la sécurité de l'infrastructure. Il faut donc organiser un équilibre entre la protection des secrets légitimes et l'accès effectif à la preuve.

La traçabilité des contenus générés par l'IA constitue une piste importante. Les techniques de marquage, d'empreinte numérique, de watermarking ou de provenance des contenus peuvent aider à identifier qu'un contenu a été généré par un système d'IA et à reconstituer son origine. Toutefois, ces techniques ne sont pas infaillibles. Elles peuvent être supprimées, contournées ou altérées. Elles posent également des questions de standardisation et d'interopérabilité. L'AI Act met en avant des obligations de transparence pour certains contenus générés ou manipulés artificiellement, mais l'efficacité de ces obligations dépendra largement de leur traduction technique et de leur adoption par les acteurs de la chaîne numérique.[5152]

2.2. Les perspectives d'évolution du régime de responsabilité des prestataires de cloud

Face aux limites constatées, l'évolution du régime de responsabilité des prestataires cloud doit poursuivre un double objectif : préserver la neutralité légitime des intermédiaires purement techniques et renforcer la responsabilité des acteurs qui disposent d'un pouvoir réel de contrôle. Une responsabilité excessive risquerait de transformer les prestataires cloud en contrôleurs généraux de tous les contenus numériques. Une irresponsabilité excessive rendrait impossible la protection effective des titulaires de droits. La solution doit donc être fondée sur une responsabilité graduée, fonctionnelle et probatoire.

Cette évolution suppose également de dépasser l'opposition entre innovation et protection. La protection de la propriété intellectuelle ne doit pas être pensée comme un obstacle à l'intelligence artificielle, mais comme une condition de confiance dans l'économie numérique. Les créateurs, les entreprises technologiques et les utilisateurs ont intérêt à disposer de règles claires, de procédures rapides et de preuves fiables. L'incertitude juridique nuit autant aux titulaires de droits qu'aux prestataires cloud, car elle augmente les risques contentieux et fragilise les investissements.[5153]

2.2.1. Vers une clarification du statut juridique du prestataire de cloud

La première piste consiste à clarifier le statut juridique du prestataire cloud selon son rôle concret. Le droit devrait distinguer au moins trois situations. La première est celle du prestataire purement infrastructurel, qui fournit des ressources techniques sans intervenir dans les contenus ni dans les modèles d'IA. Sa responsabilité devrait être limitée, sauf connaissance effective de l'atteinte et absence de réaction raisonnable. La deuxième est celle du prestataire plateforme, qui fournit un environnement technique structuré permettant le déploiement de systèmes d'IA par des tiers. Sa responsabilité devrait dépendre de ses obligations contractuelles, de ses politiques de contrôle et de sa coopération. La troisième est celle du prestataire intégré, qui fournit lui-même des services d'IA générative. Dans ce cas, des obligations renforcées de prévention, de transparence et de traçabilité peuvent être justifiées.[5154]

Cette classification permettrait d'éviter l'insécurité juridique. Elle offrirait aux titulaires de droits un cadre pour orienter leurs actions et aux prestataires cloud une visibilité sur leurs obligations. Elle permettrait aussi aux juges de raisonner à partir de

[5152] Union européenne, Règlement (UE) 2024/1689 (AI Act), précité.
[5153] Organisation Mondiale de la Propriété Intellectuelle (OMPI), Artificial Intelligence and Intellectual Property, WIPO, 2024.
[5154] C. Millard (dir.), op. cit., 2013; Union européenne, Règlement (UE) 2022/2065 (Digital Services Act), précité; Union européenne, Règlement (UE) 2024/1689 (AI Act), précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

critères concrets : degré de contrôle, rôle dans la génération, capacité de retrait, connaissance de l'atteinte, profit tiré du service litigieux et diligence après notification. Ces critères sont plus adaptés que les catégories abstraites de neutralité ou de complicité.

Une clarification du statut devrait également intégrer le mécanisme de notification et de retrait. Lorsqu'un titulaire de droits signale une violation précise, le prestataire cloud devrait disposer d'une procédure permettant de recevoir la notification, d'évaluer son caractère suffisamment motivé, de préserver les preuves, d'informer le client concerné lorsque cela est juridiquement possible, puis d'agir de manière proportionnée. L'action peut consister à suspendre l'accès au contenu, à bloquer une diffusion, à conserver les traces ou à exécuter une décision judiciaire. L'absence de procédure claire peut constituer un indice de défaut de diligence.[5155]

La notification ne doit cependant pas devenir un outil d'abus. Les contenus générés par IA peuvent susciter des contestations complexes, notamment lorsque la similarité est discutée ou lorsque des exceptions sont invoquées. Le prestataire cloud ne doit pas être incité à retirer systématiquement tout contenu au moindre signalement, au risque de porter atteinte à la liberté d'expression, à la concurrence et à l'innovation. Il faut donc prévoir des garanties procédurales : notification motivée, contre-notification, conservation de la preuve, recours judiciaire et proportionnalité des mesures.

La contractualisation constitue un deuxième levier de clarification. Les contrats cloud devraient intégrer des clauses relatives aux usages interdits en matière de propriété intellectuelle, à la conservation des preuves, à la coopération judiciaire, à la localisation des données, à la sous-traitance, à la réversibilité, aux audits et aux incidents. Ces clauses ne doivent pas se limiter à protéger le prestataire contre toute responsabilité; elles doivent organiser une chaîne de diligence. Dans les services d'IA, les contrats devraient aussi préciser les responsabilités relatives aux données d'entraînement, aux contenus générés, aux garanties de non-contrefaçon, aux mécanismes de filtrage et aux obligations d'information des utilisateurs.[5156]

2.2.2. Vers un renforcement des obligations de traçabilité, de coopération et d'auditabilité

La deuxième piste d'évolution concerne la preuve. La responsabilité ne peut être effective sans accès aux éléments techniques nécessaires à l'imputabilité. Les prestataires cloud devraient donc être soumis à des obligations raisonnables de traçabilité, adaptées à la nature du service et au niveau de risque. Il ne s'agit pas d'imposer une surveillance générale des contenus, mais de garantir que les opérations essentielles puissent être documentées en cas de litige. Cette obligation pourrait concerner les logs d'accès, les historiques de génération, les métadonnées des fichiers, les versions de modèles utilisées et les mesures prises après notification.[5157]

L'auditabilité doit devenir un principe structurant. Un service cloud ou IA qui ne conserve aucune trace exploitable crée une zone d'irresponsabilité. À l'inverse, un service documenté permet de répartir plus justement les responsabilités. L'auditabilité ne signifie pas transparence totale du code source ou des secrets industriels; elle signifie capacité à produire, sous contrôle juridique approprié, les informations nécessaires pour vérifier un fait litigieux. Des mécanismes de tiers de confiance, d'expertise sous confidentialité ou de transmission judiciaire encadrée peuvent permettre de concilier l'accès à la preuve et la protection du secret des affaires.[5158]

[5155] Union européenne, Règlement (UE) 2022/2065 (Digital Services Act), précité.
[5156] C. Millard (dir.), op. cit., 2013; A. Bensamoun et G. Loiseau, op. cit., 2021.
[5157] National Institute of Standards and Technology, AI RMF 1.0, précité; Union européenne, Règlement (UE) 2024/1689 (AI Act), précité.
[5158] National Institute of Standards and Technology, AI RMF 1.0, précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

La coopération avec les titulaires de droits et les autorités doit également être renforcée. Les prestataires cloud sont souvent les seuls à pouvoir identifier le compte, conserver les traces ou bloquer la persistance d'un contenu. Leur coopération peut donc être décisive. Cette coopération devrait être organisée par des procédures internes, des points de contact, des délais de réponse, des formats standardisés de notification et des mécanismes de conservation temporaire des preuves. Le Digital Services Act, en prévoyant des mécanismes de signalement de contenus illicites et une approche proportionnée des obligations des services intermédiaires, fournit à cet égard une source d'inspiration méthodologique.[5159]

La transparence relative aux systèmes d'IA constitue une autre exigence. Les titulaires de droits doivent pouvoir comprendre, au moins de manière générale, si leurs œuvres peuvent avoir été utilisées dans des ensembles d'entraînement ou si le système est conçu pour générer des contenus imitant des œuvres existantes. L'AI Act européen impose certaines obligations de documentation et de transparence pour les modèles d'IA à usage général, notamment en lien avec les contenus utilisés pour l'entraînement. Cette orientation ne règle pas tous les problèmes, mais elle confirme que la responsabilité future passera par la documentation des systèmes et la capacité à rendre compte des choix techniques.[5160]

La perspective d'évolution doit aussi intégrer le droit marocain. Le Maroc dispose de textes importants en matière de propriété intellectuelle, de données personnelles, de cybersécurité et de cloud, mais l'articulation entre ces régimes reste à consolider pour les situations d'IA générative. Une réforme ou des lignes directrices pourraient préciser les obligations des prestataires cloud lorsqu'ils hébergent des systèmes d'IA susceptibles de générer des contenus protégés : conservation minimale de certaines traces, coopération en cas de notification, encadrement contractuel des usages illicites, exigences de sécurité et de réversibilité, et procédures de traitement des réclamations de propriété intellectuelle.[5161]

Enfin, l'évolution du régime de responsabilité doit préserver un équilibre. Les titulaires de droits ont besoin de protection, les utilisateurs ont besoin de liberté créative, les prestataires cloud ont besoin de sécurité juridique et la société a besoin d'innovation. Le droit ne doit pas empêcher le développement de l'IA, mais il doit empêcher que l'opacité technique serve d'écran à l'irresponsabilité. La responsabilité des prestataires cloud doit donc être construite comme une responsabilité de diligence et de coopération, plus que comme une responsabilité automatique. Cette approche permet de responsabiliser les acteurs sans leur imposer une obligation impossible de contrôle permanent.[5162]

[5159] Union européenne, Règlement (UE) 2022/2065 (Digital Services Act), précité.
[5160] Union européenne, Règlement (UE) 2024/1689 (AI Act), précité.
[5161] Loi n° 2-00 relative aux droits d'auteur et droits voisins, précitée; Loi n° 05-20 relative à la cybersécurité, précitée; Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, précitée; Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services cloud, précité.
[5162] Union européenne, Règlement (UE) 2022/2065 (Digital Services Act), précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

Conclusion

La responsabilité des prestataires de cloud face aux violations de la propriété intellectuelle générées par l'intelligence artificielle révèle l'une des tensions majeures du droit numérique contemporain. Le cloud computing rend possible l'entraînement, l'exécution, l'hébergement et la diffusion des systèmes d'IA. L'intelligence artificielle générative, de son côté, multiplie les situations dans lesquelles des œuvres protégées peuvent être reproduites, imitées, transformées ou diffusées sans autorisation. Entre ces deux dynamiques, le prestataire cloud occupe une position stratégique mais juridiquement ambivalente : il n'est pas toujours l'auteur direct de l'atteinte, mais il détient souvent les moyens techniques permettant de prévenir, limiter, documenter ou faire cesser la violation.

L'analyse a montré que la difficulté principale réside dans la qualification juridique du rôle du prestataire. Lorsque celui-ci agit comme un simple fournisseur d'infrastructure, sa responsabilité doit rester limitée et subordonnée à la connaissance effective de l'atteinte ou à une faute de diligence. Lorsqu'il propose des services intégrés d'IA, contrôle les conditions de génération ou participe activement à l'organisation du service, son rôle devient plus substantiel et peut justifier des obligations renforcées. La responsabilité ne doit donc pas être pensée de manière uniforme, mais selon une logique graduée fondée sur le contrôle, la connaissance, la capacité d'intervention et la coopération.

Les régimes classiques de responsabilité civile et de propriété intellectuelle demeurent utiles, mais ils montrent leurs limites face à la complexité de l'IA et du cloud. La faute, le lien de causalité, la contrefaçon et l'imputabilité sont plus difficiles à établir lorsque les actes sont automatisés, fragmentés et distribués entre plusieurs acteurs. La violation peut résulter d'une chaîne technique dans laquelle interviennent l'utilisateur, le fournisseur du modèle, le prestataire cloud, la plateforme de diffusion et parfois plusieurs sous-traitants. Cette pluralité impose une méthode d'analyse fonctionnelle plutôt qu'une application mécanique des catégories classiques.

La preuve constitue le point décisif. Sans logs, métadonnées, historiques de requêtes, versions de modèles, traces d'accès ou mécanismes de traçabilité, la responsabilité reste théorique. Les titulaires de droits peuvent constater une atteinte sans pouvoir identifier l'auteur ni démontrer le rôle du prestataire. L'environnement cloud crée une asymétrie informationnelle qui doit être compensée par des obligations raisonnables de conservation, de coopération et d'auditabilité. Toutefois, ces obligations doivent respecter la protection des données personnelles, le secret des affaires, la sécurité des systèmes et la proportionnalité.[5163]

La réponse à la problématique peut donc être formulée ainsi : la responsabilité des prestataires de cloud en cas de violations de la propriété intellectuelle générées par l'IA doit être déterminée à partir d'une appréciation concrète de leur rôle dans la chaîne numérique et de leur comportement probatoire. Le prestataire ne doit pas être automatiquement responsable du seul fait que ses infrastructures ont été utilisées. En revanche, il peut engager sa responsabilité lorsqu'il joue un rôle actif, lorsqu'il a connaissance effective d'une atteinte précise, lorsqu'il dispose d'une capacité raisonnable d'intervention et lorsqu'il ne prend pas les mesures nécessaires pour préserver les preuves, coopérer ou limiter la persistance du dommage.

Les perspectives d'évolution du droit doivent aller vers une clarification du statut des prestataires cloud, une meilleure articulation entre propriété intellectuelle, responsabilité numérique et régulation de l'IA, ainsi qu'un renforcement des obligations de traçabilité. Le droit marocain pourrait s'inspirer des dynamiques européennes et internationales tout en

[5163] Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, précitée; CNDP, op. cit., 2023; National Institute of Standards and Technology, AI RMF 1.0, précité.

tenant compte de ses propres instruments, notamment la loi n° 2-00 sur les droits d'auteur et droits voisins, la loi n° 05-20 sur la cybersécurité, la loi n° 09-08 sur les données personnelles et le décret n° 2-24-921 relatif aux prestataires cloud dans les environnements sensibles. L'enjeu n'est pas seulement de sanctionner les violations, mais d'organiser une gouvernance préventive des risques de propriété intellectuelle dans les environnements cloud et IA.[5164]

En définitive, l'intelligence artificielle générative oblige le droit à repenser la responsabilité au-delà de l'auteur humain direct. Le cloud oblige, quant à lui, à penser la preuve au-delà du support matériel visible. La rencontre entre ces deux technologies impose un droit plus fonctionnel, plus probatoire et plus coopératif. La responsabilité des prestataires cloud doit être construite comme une responsabilité de diligence numérique : une responsabilité qui n'écrase pas l'innovation, mais qui empêche que la complexité technique devienne un refuge pour l'irresponsabilité.

bibliographie

(1) Abbott, R. (2020). The reasonable robot: Artificial intelligence and the law. Cambridge University Press.

(2) Aplin, T., & Bently, L. (2020). Global mandatory fair use: The nature and scope of the right to quote copyright works. Cambridge University Press.

(3) Bensamoun, A., & Loiseau, G. (2021). Droit du numérique : Contrats, innovation, données et gouvernance. Eyrolles.

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

(5) Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.

(6) 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 du Royaume du Maroc.

(7) Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique. Journal officiel de l'Union européenne.

(8) Dusollier, S. (2020). Droit d'auteur et protection des œuvres dans l'univers numérique. Larcier.

(9) Ginsburg, J. C., & Budiardjo, L. A. (2019). Authors and machines. Berkeley Technology Law Journal, 34(2), 343-448.

(10) Loi n° 2-00 relative aux droits d'auteur et droits voisins, promulguée par le Dahir n° 1-00-20 du 15 février 2000, telle que modifiée et complétée. Bulletin Officiel du Royaume du Maroc.

(11) Loi n° 05-20 relative à la cybersécurité, promulguée par le Dahir n° 1-20-69 du 25 juillet 2020. Bulletin Officiel du Royaume du Maroc.

(12) 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. Bulletin Officiel du Royaume du Maroc.

(13) Millard, C. (Ed.). (2013). Cloud computing law. Oxford University Press.

(14) National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce.

[5164] Loi n° 2-00 relative aux droits d'auteur et droits voisins, précitée; Loi n° 05-20 relative à la cybersécurité, précitée; Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, précitée; Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services cloud, précité.

ISSN:2509-0291
DOI
http://doi.org/10.63585/VLQV1532
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
Volume 11 issue 05
N:66 OCTOBRE 2026
www.Droitetentreprise.com
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

(15) Organisation Mondiale de la Propriété Intellectuelle. (2024). Artificial intelligence and intellectual property. WIPO.

(16) Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.

(17) Sirinelli, P. (2022). Propriété littéraire et artistique. Dalloz.

(18) Union européenne. (2022). Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques (Digital Services Act). Journal officiel de l'Union européenne.

(19) Union européenne. (2024). Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act). Journal officiel de l'Union européenne.

(20) Vivant, M., & Bruguière, J.-M. (2023). Droit d'auteur et droits voisins. Dalloz.

(21) World Intellectual Property Organization. (1996). WIPO Copyright Treaty. WIPO.

(22) World Trade Organization. (1994). Agreement on trade-related aspects of intellectual property rights. WTO.