



Protection de l'identité numérique à l'ère du deepfake via le droit d'auteur, faut-il y croire ?

Actualité législative publié le 19/07/2025, vu 155 fois, Auteur : [YAV & ASSOCIATES](#)

Traditionnellement, la protection juridique de l'identité en ligne s'appuyait sur le droit à l'image et sur les actions en diffamation ou en usurpation d'identité. Quid aujourd'hui à l'ère des contenus deepfakes?

Joseph YAV KATSHUNG

Professeur des Universités, Avocat ; Mandataire Agréé en Propriété Industrielle ; Arbitre Agréé auprès du CAMC/O et Membre du comité de l'AIFOD [*Artificial Intelligence for Developing Countries Forum*]

1. Liminaires

L'avènement des *deepfakes*^[1] - traduit par « hypertrucage » en français, - des vidéos ou enregistrements audio falsifiés par l'IA - pose une menace croissante pour la réputation, la vie privée et la sécurité des individus et la notion d'identité personnelle se retrouve bouleversée. En quelques clics, il devient possible de créer un faux discours d'une personnalité publique ou de générer des images, des vidéos indiscernables de la réalité et des scènes diffamatoires à l'encontre d'un particulier. Cette technologie, qui s'appuie sur l'intelligence artificielle, soulève une question : *comment protéger efficacement l'identité numérique d'un individu face à ces manipulations sophistiquées ?*

Traditionnellement, la protection juridique de l'identité en ligne s'appuyait sur le droit à l'image et sur les actions en diffamation ou en usurpation d'identité. Or, ces leviers montrent leurs limites face à la rapidité de diffusion et à la difficulté d'attribution des contenus *deepfake*. Le droit d'auteur, souvent considéré comme cantonné à la création artistique, offre pourtant un potentiel inédit pour encadrer la reproduction, la modification et la diffusion non autorisée de l'identité numérique (visage, voix, signature artistique). Cette note propose d'explorer l'utilisation du droit d'auteur comme nouvel instrument de sauvegarde de l'identité des personnes physiques et morales en ligne, ses atouts et ses limites. Cela est d'autant plus qu'urgent car, les réseaux sociaux sont devenus la principale source d'information pour des millions d'Africains, ce qui amplifie la viralité des fausses nouvelles, souvent sans vérification préalable. Sans garde-fous, les *fakes news* et les *deepfakes* y trouvent un terrain fertile. Or, la plupart des pays africains restent sous-équipés en matière de réglementation, de compétences et d'innovations liées à l'IA pour

contrer ces menaces émergentes.

2. Contexte et état de l'art

2.1 Définitions et enjeux de l'identité numérique

La notion d'identité numérique repose sur un socle juridique en constante évolution. Classiquement, l'identité est appréhendée comme l'ensemble des traits ou caractéristiques qui, au regard de l'état civil, permettent de reconnaître une personne et d'établir son individualité au regard de la loi. Elle recoupe des identifiants tels que le nom, le prénom, la date de naissance, la filiation, ...

Avec les évolutions technologiques, ces éléments se sont multipliés. Un profil Facebook, un avatar de jeu vidéo, un double virtuel créé à partir des traces de navigation, sont autant de données qui ont abouti à l'émergence dans la doctrine d'une identité électronique, génétique, numérique ou encore biométrique. Certains auteurs traitent même « des » identités pour viser, semble-t-il, chacun des pans de la vie d'un individu.[2] Or, ces réalités relèvent-elles vraiment de l'identité au sens juridique du terme ? Existe-t-il une identité numérique ? Ces questions présentent un grand intérêt car, si l'identité est un outil précieux, c'est parce qu'elle renvoie à une réalité d'une grande fiabilité dont l'État est le garant. Sans cela, l'identité devient un ensemble de données comme un autre. Elle ne peut alors plus être ce référent suscitant la confiance, unique et incontournable. Ce faisant, elle perd son rôle en termes de singularisation des personnes et de sécurisation des échanges.

La notion d'identité numérique mérite donc d'être questionnée avant de chercher à déterminer quel cadre juridique il serait nécessaire de lui appliquer. L'explosion des réseaux sociaux et plus globalement, d'internet, a favorisé la multiplication des données personnelles sur internet et leur circulation sur la toile. Tout utilisateur dispose aujourd'hui d'une identité à plusieurs dimensions : à la fois personnelle, et fait tout récent, d'une identité numérique qu'il doit savoir et pouvoir gérer et protéger pour ne pas se laisser dépasser par la collecte et le stockage de données personnelles. Dans cette note, l'identité numérique regroupe l'ensemble des traces et représentations d'un individu sur Internet. Elle se construit à travers les contenus qu'une personne publie, les interactions sociales, ainsi que les métadonnées associées. Au-delà de la simple « e-réputation », elle inclut la reconnaissance biométrique, visage et voix, employée par les technologies de vérification d'accès.

Le maintien d'une identité numérique fiable est essentiel pour sauvegarder la vie privée, limiter les risques d'usurpation d'identité et préserver la confiance dans les échanges en ligne. L'apparition des *deepfakes* fait peser une menace nouvelle, la création et la diffusion de contenus fallacieux à grande échelle, susceptibles de porter atteinte à l'intégrité physique, morale et professionnelle des victimes.

2.2 Principes techniques et impacts sociétaux des deepfakes

Les *deepfakes* se fondent sur des algorithmes de type GAN (*Generative Adversarial Network*) [3] capables de synthétiser des images et des voix ultraréalistes. Selon cette technologie, deux algorithmes s'entraînent mutuellement, l'un tente de fabriquer des contrefaçons aussi fiables que possible ; l'autre tente de détecter les faux. De cette façon, les deux algorithmes s'améliorent ensemble au fil du temps grâce à leur entraînement respectif. Plus le nombre d'échantillons disponibles augmente, plus l'amélioration de ceux-ci est importante. Les progrès rapides de ces modèles permettent aujourd'hui de dupliquer une personne à partir d'un jeu de données limité, parfois quelques secondes d'enregistrement audio ou quelques photographies.

Les conséquences dépassent l'intoxication politique ou la diffusion de fausses informations. Des cas de sextorsion, d'escroquerie à la voix et de montages satiriques non consentis se multiplient. Les victimes peinent à faire retirer ces contenus, car les plateformes tardent à détecter automatiquement les *deepfakes* et le mal est fait ; et les procédures juridiques classiques sont longues et mal adaptées à la nature algorithmique des atteintes. En effet, le droit à l'image interdit l'exploitation commerciale d'une photographie ou d'une vidéo sans le consentement de la personne, mais il ne prend pas en compte les imitations synthétiques produites par algorithme. De même, les actions en diffamation exigent la preuve d'une fausse allégation portant atteinte à la réputation, ce qui ne couvre pas les montages silencieux ou les contenus entièrement fabriqués. Enfin, la responsabilité des plateformes se limite souvent à un simple retrait sous notification, sans obligation de détecter proactivement les *deepfakes*. Ces lacunes ouvrent un espace dans lequel les auteurs de contenus malveillants peuvent agir en toute impunité.

3. Le droit d'auteur au service de l'identité numérique : fondements et applicabilité à l'identité

3.1 Principes fondamentaux du droit d'auteur

Le droit d'auteur protège les œuvres de l'esprit originales : textes, images, vidéos, compositions musicales, performances. Il confère à l'auteur un monopole d'exploitation sur son œuvre, comprenant le droit de reproduction, de représentation, d'adaptation et de distribution. En l'absence de cession de droits, toute utilisation non expressément autorisée constitue une contrefaçon.

En droit congolais, la protection naît automatiquement dès la création de l'œuvre, sans formalité. C'est ce qui ressort des articles 1 et 2 de l'Ordonnance-loi n°86-033 du 5 avril 1986 portant protection des droits d'auteurs et droits voisins.[4] L'auteur dispose de droits patrimoniaux (cession, rémunération) et moraux (paternité, respect de l'intégrité). Ces prérogatives peuvent s'appliquer à la forme numérique d'une identité : photographies de portrait, enregistrements vocaux, avatar iconique.

3.2 Déclinaison au service de l'identité numérique

L'idée centrale consiste à qualifier la représentation numérique d'un individu - photos, vidéos, synthèses vocales - d'œuvre de l'esprit immatérielle. En enregistrant chaque image ou séquence vocale dans un registre de droits d'auteur ou via la blockchain[5] pour l'horodatage[6], on crée une preuve d'antériorité et d'originalité. Toute reproduction ou modification sans licence devient alors susceptible de poursuites pour contrefaçon.

L'approche par le droit d'auteur offre un cadre souple et puissant, mais elle n'est pas sans limites. D'une part, tous ne peuvent pas revendiquer la qualité d'auteur pour leur simple image. D'autre part, la mise en œuvre technique - *blockchain*, *watermarking* - nécessite des compétences et un coût non négligeable. Il importe donc de développer des outils accessibles et des standards interopérables.

La coopération entre États, plateformes et législateurs apparaît cruciale. À l'échelle européenne, la réforme du droit d'auteur devrait intégrer explicitement la notion d'identité numérique et prévoir des sanctions adaptées au caractère automatisé des *deepfakes*.

4. Le droit d'auteur au service de l'identité numérique : Le Danemark et sa proposition de loi *deepfake*

4.1. Contexte et objectifs

Face à la montée des *deepfakes*, le Parlement danois a élaboré un projet de loi visant à qualifier les traits biométriques comme œuvres protégées, instaurer un droit de retrait et d'indemnisation, responsabiliser juridiquement les plateformes de diffusion. Concrètement, de par sa proposition de la refonte de sa loi sur le droit d'auteur, le gouvernement danois entend reconnaître explicitement les traits biométriques - visage, voix et gestuelle - comme œuvres de l'esprit, soumises à autorisation préalable avant toute diffusion numérique réaliste non consentie. L'objectif est d'offrir aux individus un droit de retrait effectif et un recours en dommages-intérêts quand leur identité est détournée par des *deepfakes*.

En assimilant les caractéristiques biométriques à des « œuvres de l'esprit », le texte octroie à chaque individu un droit exclusif de reproduction, de représentation et d'adaptation de son visage, de sa voix ou de ses gestes. Cette qualification juridique permettrait notamment d'engager des poursuites pour contrefaçon dès lors qu'une imitation numérique réaliste est diffusée sans autorisation écrite. Les droits moraux, tels que le respect de l'intégrité de l'œuvre, viennent compléter ce dispositif en interdisant toute altération portant atteinte à la dignité de la personne.

Pour garantir l'effectivité de ces droits, la loi danoise prévoit l'instauration d'un registre public *horodaté*^[7] sur blockchain^[8], dans lequel chaque représentation biométrique est enregistrée sous forme de hash cryptographique. Ce procédé infalsifiable permet de prouver l'antériorité des dépôts et de retracer toute diffusion non autorisée. Par ailleurs, l'utilisation de *watermarking*^[9] invisible dans les médias audiovisuels renforce la traçabilité des contenus en y insérant des marqueurs discrets détectables par des algorithmes spécifiques. Enfin, les certificats numériques issus d'une infrastructure de clés publiques assurent l'authenticité et l'intégrité des fichiers originaux, créant une chaîne de confiance entre le créateur de l'œuvre biométrique et les plateformes de diffusion.

Adopté à une large majorité parlementaire, le projet danois impose aux hébergeurs de retirer toute imitation non autorisée sous vingt-quatre heures après notification, sous peine d'amendes pouvant atteindre 5% de leur chiffre d'affaires annuel. Le texte prévoit cependant des exceptions pour la satire, la parodie ou la critique, afin de préserver la liberté d'expression et la mission d'information des médias. Par ce dispositif, le Danemark entend non seulement offrir aux victimes un recours rapide et dissuasif, mais aussi impulser à Bruxelles l'élaboration d'une directive européenne harmonisée sur la protection de l'identité numérique par droit d'auteur.

Notons toutefois que cette initiative danoise s'inscrit dans un contexte européen pour le moins mouvant. L'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) examine actuellement des demandes d'enregistrement de visages humains comme marques, avec des décisions contrastées qui révèlent l'absence de consensus juridique. Plusieurs modèles néerlandais ont ainsi obtenu la protection de leurs portraits photographiques, tandis que d'autres demandes ont été rejetées pour manque de caractère distinctif.^[10] Barna Arnold Keseru (2024) dans une étude universitaire^[11] recense pourtant pas moins de 57 marques de portraits masculins, 23 marques de portraits féminins et 3 d'enfants actuellement protégées en tant que marques de l'Union européenne. Loin d'être anodins, ces chiffres montrent bien qu'un marché de l'identité commercialisée est déjà actif.

4.2. Implications de la loi danoise sur le droit d'auteur

a. Étendue des droits et reconnaissance des traits biométriques

La réforme étend le droit d'auteur aux caractéristiques personnelles - visage, voix et gestuelle - en les assimilant à des « œuvres de l'esprit ». Chaque citoyen danois acquiert ainsi un monopole d'exploitation sur sa propre identité numérique : reproduction, représentation et adaptation de son image ou de sa voix ne sont plus possibles sans son consentement préalable.

b. Renforcement des mécanismes d'application

Pour concrétiser ces droits, la loi impose aux plateformes et hébergeurs l'obligation de retirer tout *deepfake* non autorisé sous 24 heures après notification ; la mise en place d'un registre public dématérialisé des enregistrements biométriques protégés et ; l'exposition à des amendes sévères (jusqu'à 5 % du chiffre d'affaires annuel) en cas de manquement à leurs obligations de retrait et de diligence raisonnable.

c. Exceptions pour préserver la liberté d'expression

Le texte encadre strictement son périmètre pour éviter la censure automatique dont les satire, parodie et critique artistique sont expressément exclues du champ d'application ainsi que toute utilisation à but informatif ou journalistique, dès lors qu'elle ne porte pas atteinte à l'intégrité physique ou morale, demeure autorisée.

d. Implications internationales de la loi danoise

La reconnaissance des traits biométriques comme « œuvres de l'esprit » au Danemark crée un précédent législatif au sein de l'Union européenne. En étant le premier État-membre de l'UE à inscrire la protection des traits biométriques dans le droit d'auteur, le Danemark entend impulser une directive européenne harmonisée^[12]. Cette initiative devrait nourrir les travaux autour du Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) appelé « *Digital Services Act* » et du Règlement sur l'intelligence artificielle (*Artificial Intelligence Act* ou *AI Act*), en incitant Bruxelles à intégrer explicitement la notion de droit d'auteur « personnalisé » pour contrer les *deepfakes* à l'échelle communautaire. Ces dispositions redéfinissent le paradigme de la protection de l'identité numérique, alliant les prérogatives classiques du droit d'auteur à des mécanismes innovants de traçabilité et de responsabilité algorithmique.

Le texte danois offre un modèle exportable car il sert de référence pour concevoir des licences-types et des obligations de retrait rapide en cas de violation, réduisant le risque de fragmentation réglementaire au sein du marché unique. Cela a un impact sur les acteurs technologiques mondiaux dont les plateformes globales (Meta, Google, TikTok...) qui devront, pour rester

présentes au Danemark, mettre en place des systèmes de détection et de suppression automatisée des contenus *deepfake* non autorisés. Aussi, cette obligation contractuelle contraindra ces acteurs à adopter des solutions universelles[13] qui tendront à se généraliser sur l'ensemble de leurs services internationaux.

5. Influence sur les pays africains : Transposition en RDC et perspectives africaines

L'approche par droit d'auteur offre un cadre à la fois souple et puissant, mais elle nécessite un engagement financier et technique conséquent de la part des États et des acteurs privés. Pour être pleinement opérationnel, le dispositif doit s'appuyer sur des standards ouverts de *watermarking* et d'*horodatage* ainsi que sur des programmes de formation ciblés. La coopération transnationale, qu'elle passe par une directive européenne ou par un protocole africain, s'avère cruciale pour éviter la fragmentation réglementaire et garantir une protection effective dans un environnement numérique globalisé. Sinon, en l'absence d'un droit à l'image numérique explicite, les victimes doivent se rabattre sur des lois existantes (ex : diffamation, escroquerie), souvent inadaptées aux *deepfakes*. L'initiative danoise, en créant un cadre juridique clair, met en lumière ce vide en Afrique et pourrait inciter à réfléchir à des dispositifs similaires pour protéger les citoyens africains[14]. Au niveau continental, l'Union africaine s'est dotée en juillet 2024 d'une *Stratégie continentale sur l'IA (2025-2030)*[15], prônant une utilisation éthique de ces technologies et la minimisation des risques pour les droits humains. Ce document-cadre, aligné sur les valeurs de dignité, de respect des droits de l'Homme et de bien-être des populations, recommande aux pays membres d'adopter des législations encadrant l'usage de l'IA et de ses dérivés. La sensibilisation aux *deepfakes* y est mentionnée comme une urgence, de même que le besoin de développer des solutions technologiques de détection. Cependant, la mise en œuvre concrète de ces recommandations reste lente et inégale selon les pays.

En RDC, la protection de l'identité numérique repose aujourd'hui sur un Code de la propriété intellectuelle centré sur les œuvres traditionnelles, ainsi que sur l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique[16]. L'usurpation d'identité est prévue et sanctionnée par l'article 351 du code du numérique qui incrimine le fait d'usurper l'identité d'autrui ou les données permettant de s'attribuer faussement et de manière illicite l'identité d'autrui dans le but de troubler sa tranquillité, de porter atteinte à son honneur, à sa considération ou à ses intérêts. De même, celui qui aura transféré, possédé ou utilisé un moyen de s'identifier à une autre personne dans l'intention de commettre l'infraction, d'aider ou d'encourager une activité illégale est puni d'une peine de deux à cinq ans de servitude pénale et/ou d'une amende de 5 à 100 millions de francs congolais. À côté de l'infraction d'usurpation d'identité, le code du numérique sanctionne sous une autre forme l'utilisation frauduleuse des éléments d'identification dans le but de tromper les usagers d'un service de communication électronique. Ainsi, l'article 349 punit au titre de tromperie, le fait d'utiliser les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles.

Les cas d'usurpation d'identité numérique ne sont pas rares, en RDC par exemple, de faux comptes profitant de l'identité d'autrui proliféraient, et diffusaient des rumeurs ou des discours mensongers. Avec la venue du *Code du numérique (2023)*[17], l'accès non autorisé à des données personnelles, l'usurpation d'identité, la tromperie en ligne, les *fake news* et la

diffamation sont désormais punis par la loi. Cette avancée juridique en RDC montre une prise de conscience sur la nécessité de protéger l'identité numérique et la vérité factuelle. Une loi spécifiquement centrée sur les *deepfakes* viendrait compléter ce dispositif en couvrant les cas où la voix ou le visage d'une personne sont reproduits artificiellement. Elle offrirait aux victimes congolaises un recours légal pour exiger le retrait de vidéos/voix contrefaites les impliquant, là où le Code du numérique actuel vise plus largement les *fake news* et l'usurpation d'identités sur les réseaux.

En somme, l'approche consistant à accorder un droit de regard et de veto aux individus sur leur double numérique soulève des enjeux complexes mais essentiels. Elle cherche à *humaniser* la révolution de l'IA en y inscrivant des limites morales – le respect de l'autre, de sa voix, de son visage, de son identité unique. Pour l'Afrique et la RDC, ces considérations éthiques se doublent de contextes pratiques difficiles, mais ignorer la question serait prendre le risque de subir de plein fouet les dérives de l'IA sans filet de sécurité. L'équation éthique à résoudre est universelle : *comment tirer parti des technologies d'IA tout en protégeant la vérité et la dignité humaine à l'ère du faux indiscernable ?*

6. Que conclure ?

Face à la montée en puissance des *deepfakes*, il est urgent de repenser la protection de l'identité numérique. L'idée de mobiliser le droit d'auteur pour la défendre face aux *deepfakes* séduit par sa promesse de robustesse juridique. En qualifiant le visage, la voix ou la gestuelle d'« œuvres de l'esprit », on crée un monopole d'exploitation qui interdit toute reproduction non autorisée et offre un recours pour contrefaçon. Ce levier permettrait de responsabiliser plus fortement les plateformes et de garantir à chacun un droit de retrait rapide.

Pourtant, plusieurs obstacles viennent tempérer cet optimisme. D'abord, la notion même d'originalité, pilier du droit d'auteur, peine à s'appliquer aux données biométriques ; un visage « commun » ou une voix standardisée résisteront difficilement à la qualification d'œuvre. Ensuite, l'efficacité du dispositif repose sur des infrastructures coûteuses (*blockchain*, *watermarking* invisible, *forensic IA*) et sur la formation de juges et d'experts capables d'analyser techniquement les fichiers. En avons-nous les moyens, surtout dans nos pays d'Afrique subsaharienne ? *That is the question !* Bien plus, la transposition d'un tel régime exige une coordination législative internationale pour éviter que les *deepfakes* circulent d'un pays à l'autre sans contraintes. Enfin l'on se pose la question de savoir si *l'initiative danoise, bien qu'animée d'intentions protectrices, pourrait paradoxalement accélérer la marchandisation de l'identité personnelle ?* A ce sujet, Marion Zilio (2018), observait déjà en 2018 que « *le visage ne nous appartient plus : il est la propriété de plates-formes capitalistes* »^[18]. En transformant l'apparence physique en propriété intellectuelle, la proposition danoise risque donc de légitimer conceptuellement l'exploitation commerciale des identités, même si elle vise initialement à la contrôler.

Hormis ces défis, l'extension du droit d'auteur ne peut être pensée en vase clos. Elle doit s'articuler avec le droit à l'image, le droit de la vie privée et la responsabilisation des hébergeurs. Les solutions purement juridiques se révèlent souvent insuffisantes face à la rapidité et à l'opacité des réseaux de distribution de contenus. Des technologies complémentaires - détection

algorithmique, filigranes numériques, certificats d'authenticité - sont indispensables pour rendre concrète la protection.

Alors, faut-il y croire ? Le droit d'auteur offre un cadre novateur et potentiellement dissuasif pour lutter contre les *deepfakes*, à condition de le concevoir comme un outil parmi d'autres. Pour qu'il devienne véritablement efficace, il doit être soutenu par une stratégie globale alliant régulation technologique, coopération internationale et renforcement des compétences. En l'état, le droit d'auteur n'est pas une panacée, mais un levier précieux au sein d'un arsenal plus vaste. *Mais osons quand même !*

[1] Un *deepfake* est une vidéo, une image ou un enregistrement audio modifié ou créé à l'aide de l'intelligence artificielle. Ces créations semblent réalistes, mais sont en réalité des représentations trompeuses de personnes ou d'événements qui n'ont jamais eu lieu. Les *deepfakes* constituent désormais une cybermenace redoutable, impactant aussi bien les sphères juridiques, médiatiques, politiques que financières. Lire : Bénédicte Deleporte, *Deepfakes : Opportunités technologiques et risques juridiques*, octobre 2024,

[2] Eynard, Jessica, *L'identité numérique : quelle définition pour quelle protection ?* Larcier, Paris, Janvier 2020

[3] Les GANs, en français « *réseaux antagonistes génératifs* » sont des modèles d'IA générative basés sur l'apprentissage non supervisé. Ils reposent sur la compétition de deux réseaux de neurones antagonistes : un générateur et un discriminateur. Le principe est simple, le générateur génère de nouvelles données, puis le discriminateur essaie de déterminer si cette production est ou non synthétique. L'objectif du générateur est de tromper le discriminateur, son travail s'arrête lorsque ce dernier ne parvient plus à distinguer entre matériel réel et généré. Prenons un exemple, et imaginons qu'un faussaire et un policier rattaché au service de lutte contre les contrefaçons soient enfermés dans la même pièce. Pour passer le temps, le faussaire fabrique de faux billets, qu'il mélange ensuite à de vrais billets avant de demander au policier d'analyser tous ces billets, les vrais comme les faux. Tant que le policier parvient à distinguer des faux billets, le processus se répète, ce qui permet au faussaire d'affiner ses copies de plus en plus. L'œil du policier s'aiguise également, mais arrive un moment où même lui finit par se faire avoir. Lire à ce sujet :

Moez Krichen, *Les Generative Adversarial Networks*, Laboratoire ReDCAD, Université de Sfax, Tunisie, <https://hal.science/hal-04140057v1/document>

[4] Art.1.-L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous... Art.2.- L'œuvre est réputée créée, indépendamment de toute divulgation publique, du seul fait de la réalisation, même inachevée, de la conception de l'auteur.

[5] La blockchain permet d'inscrire de manière infalsifiable l'existence d'une œuvre numérique à une date précise. En hachant la donnée audiovisuelle (portrait ou voix) et en publiant cet hash sur une chaîne publique, on génère un certificat inviolable. Cette preuve peut être produite devant un tribunal pour établir la violation des droits patrimoniaux ou moraux de l'auteur.

[6] Le *watermarking* ou le marquage numérique invisible consiste à insérer des informations dans le contenu audiovisuel, détectables par des algorithmes de lecture spécifique. Ces filigranes peuvent lier chaque diffusion à un détenteur de droits, dissuadant les plateformes de laisser circuler des *deepfakes* non autorisés. De plus, l'usage de certificats numériques garantit l'authenticité des fichiers originaux.

[7] En matière de droit d'auteur, la blockchain offre une fonctionnalité essentielle : *l'horodatage*. Lorsqu'un créateur dépose un document (croquis, photo, description, etc.) sur la blockchain via un service dédié, ce dépôt se voit attribuer une date précise, et cette date ne pourra plus être contestée. On parle alors d'« ancrage ». Cette technique présente plusieurs avantages : *La fiabilité de la preuve* : la nature même de la blockchain rend cette date très difficile à contester, puisque le réseau décentralisé authentifie l'enregistrement ; *La simplicité d'accès* : contrairement à certaines formalités administratives pouvant exiger un déplacement chez un notaire ou une enveloppe Soleau, l'ancrage blockchain peut s'effectuer en ligne, à tout moment et ; *La valeur juridique grandissante*. Grâce à la reconnaissance de cette technologie par les tribunaux, prouver la paternité d'une œuvre (dessin, modèle, partition, texte, etc.) devient un processus à la fois rapide et solide. Lire: Etienne Deshoulières, Comment la blockchain révolutionne la protection des œuvres, 16 Avr 2025 , <https://www.deshoulieres-avocats.com/comment-la-blockchain-revolutionne-la-protection-des-oeuvres/>

[8] La blockchain (ou « chaîne de blocs ») est un registre, *une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie*[8].

[9] Technique bien connue dans la protection des droits d'auteurs, le tatouage numérique appelé *filigrane* ou *watermark* en anglais, est une technologie de pointe qui consiste à intégrer des données invisibles dans des fichiers numériques (tels que des images, des vidéos, des documents ou des fichiers audio) pour préserver leur origine, leur propriété et leur intégrité. Ces informations intégrées peuvent servir à diverses fins, telles que la traçabilité, la garantie d'intégrité et la détection de l'utilisation non autorisée ou détournée des contenus. À l'ère de l'IA générative les contenus générés se propagent instantanément, sont de plus en plus réalistes et l'information est souvent consommée sans discernement. La question de la véracité, de l'intégrité et de la traçabilité des contenus devient donc plus que jamais cruciale. La mise en place de technologies avancées tel que le tatouage numérique est désormais considérée comme une nécessité incontournable. Cette solution offre une réponse efficace aux défis posés par la multiplication des contenus générés par l'IA, dont la prolifération de *fakenews* et *deepfakes*, tout en permettant d'intégrer un droit d'opposition (« *opt-out* ») face à l'utilisation abusive des données destinées à entraîner les intelligences artificielles.

[10] UGGC Avocats, Le visage, un signe figuratif comme un autre ? L'EUIPO se positionne, 20 février 2025, <https://www.uggc.com/le-visage-un-sign-figuratif-comme-un-autre-leuipo-se-positionne/>

[11] Barna Arnold Keseru, Trademark protection for faces? A comprehensive analysis on the benefits and drawbacks of trademarks and the right to facial image, in Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 2024/1, June 2024

[12] Copenhague compte user de sa présidence du Conseil de l'UE pour proposer une directive commune, renforçant ainsi le régime européen de l'*AI Act* et du *Digital Services Act* par une dimension « droit d'auteur personnalisé ».

[13] Comme *watermarking*, scans OCR/face recognition et API d'horodatage blockchain,

[14] Certains États africains commencent à réagir contre la désinformation numérique. Par exemple, l'Ouganda a révisé en 2022 sa loi contre la cybercriminalité pour pénaliser la diffusion de fausses informations, y compris les *deepfakes*, et l'usurpation d'identité en ligne. Cette modification interdit également l'accès non autorisé aux données personnelles et le partage de données sensibles sur les enfants. C'est une première étape vers la reconnaissance du problème. D'autres pays, comme le *Kenya* ou le *Nigeria*, ont débattu de projets de loi contre les *fake news* et les trucages malveillants, conscients des dangers pendant les élections notamment.

[15][https://au.int/sites/default/files/documents/44004-doc](https://au.int/sites/default/files/documents/44004-doc_FR_Strategie_Continentale_sur_lIntelligence_Artificielle_3.pdf)
FR_Strategie_Continentale_sur_lIntelligence_Artificielle_3.pdf

[16] Lire a ce sujet, Balaise Loleka Ramazani, Le droit congolais face aux enjeux de protection de

[17] L'ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique en RDC.

[18] Marion Zilio, Faceworld, le visage au XXI^e siècle, Paris, PUF, 2018