



LE METAVERS METAVERSE

LE METAVERS : DES OPPORTUNITES ECONOMIQUES MAJEURES

- Le terme métavers est apparu en 1992 sous la plume d'un auteur de science-fiction, Neal Stephenson. Le concept s'est ensuite développé dans des jeux vidéo (Fortnite, Second Life) ainsi qu'au cinéma (Matrix, The thirteen floor) avant de cristalliser l'attention quand Mark Zuckerberg a annoncé à l'automne 2021 que Facebook changeait de nom pour devenir Meta. A l'heure du Web 3.0, beaucoup pensent que les métavers, alliés à la technologie blockchain, seront les éléments clés de l'Internet de demain.
- Selon le Conseil de l'UE, le métavers peut être défini comme « un monde virtuel, immersif, et persistant en 3D où les personnes interagissent au moyen d'un avatar pour réaliser un large éventail d'activités ». Il n'existe pas un seul métavers, mais de nombreuses plateformes de métavers (The Sandbox, Decentraland ou encore Roblox).
- Les entreprises ont tout intérêt à investir massivement dans ce nouveau monde qui offre des opportunités économiques majeures.

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Australie, Brésil, Espagne, Etats-Unis, France, Grèce, Italie, Royaume-Uni.

METAVERSE: MAJOR ECONOMIC OPPORTUNITIES

- *The term metaverse first appeared in 1992 under the pen of a science fiction author, Neal Stephenson. The concept was then developed in video games (Fortnite, Second Life) and movies (Matrix, The thirteen floor) before coming under the spotlight in the fall of 2021 when Mark Zuckerberg announced that Facebook was changing its name to Meta. At the time of Web 3.0, many believe that metaverses, along with blockchain technology, will be a key element of tomorrow's Internet.*
- *According to the Council of the EU, the metaverse can be described as "an immersive and constant virtual 3D world where people interact by means of an avatar to carry out a wide range of activities". There is not just one metaverse, but many metaverse platforms (e.g. The Sandbox, Decentraland, Roblox).*
- *Businesses have every interest in investing massively in this new world which offers major economic opportunities.*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Australia, Brazil, France, Greece, Italy, South Africa, Spain, United Kingdom, United States.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

<https://lexing.network>







ALAIN BENSOUSSAN

Fondateur et président
 de Lexing Alain Bensoussan-Avocats
 Fondateur et président
 du réseau Lexing®

Founder and Managing Partner
 of Lexing Alain Bensoussan-Avocats
 Founder and President
 of the Lexing® network





Métavers et signatures électroniques

▪ Définir le métavers, issu de la combinaison de plusieurs technologies émergentes, n'est pas chose aisée. Certains estiment que le métavers, appelé à succéder à internet tel que nous le connaissons aujourd'hui, est déjà présent sous diverses formes, d'autres qu'il n'existe pas encore. Quoi qu'il en soit, rien ne s'oppose à l'utilisation de signatures électroniques dans le métavers, à condition que les parties à la transaction respectent bien les exigences qui s'imposent pour les signatures électroniques classiques. Des ajustements pourraient néanmoins être nécessaires compte tenu du fait que, dans le métavers, les signataires interagissent par avatars virtuels interposés sur des plateformes et non via un logiciel de signature comme c'est le cas actuellement. Cependant, on ne peut écarter l'hypothèse où un tribunal (placé assez haut dans la hiérarchie judiciaire pour que sa décision ait du poids) mette un frein au développement de la signature électronique dans le métavers en s'y opposant dans une espèce dont il aurait été saisi et pour laquelle il aurait à appréhender sa validité au regard d'une législation obsolète. Moralité : les législateurs vont devoir mettre à jour les lois sur les transactions électroniques afin de garantir le plein effet de la signature électronique de documents par voie électronique, que ce soit via la version actuelle d'internet ou sa version future possible, le métavers.

Pourquoi est-il difficile de définir le métavers ?

▪ Alors que le Métavers avec un « M » majuscule fait généralement référence au produit de la société Meta Platforms, Inc. (anciennement connue sous le nom de Facebook, Inc.) **(1)**, il est plus exact de parler de « métavers » avec un « m » minuscule et au pluriel, car nul ne peut dire encore ce qu'est exactement un métavers ni combien il y en aura.

▪ Tentons toutefois d'en élaborer une définition de travail : un métavers est une version d'internet (ou d'un autre réseau plus petit) constituée d'un monde simulé auquel les personnes prennent part au moyen d'avatars numériques grâce à des technologies de réalité virtuelle et de réalité augmentée. Il peut être composé de divers éléments, dont des dispositifs améliorant virtuellement notre réalité physique (casques et gants de réalité virtuelle) et des espaces simulés persistants, c'est-à-dire qui continuent d'exister dans le temps (salles de conférence, espaces sociaux, voire des mondes entiers). **(2)**

▪ Certains considèrent que les métavers existent déjà à travers des jeux vidéo en ligne qui intègrent des mondes persistants, comme Second Life **(3)** ou Minecraft **(4)**, ou qu'ils ne seront qu'une version améliorée des logiciels de téléconférence où les gens n'interagiront plus cette fois-ci via un chat vidéo, mais via des avatars virtuels, par exemple dans les salles de travail Meta Horizon **(5)** et qu'au fil du temps, un des métavers pourrait s'imposer, effacer les autres et devenir ainsi la future version d'internet. **(6)**

▪ D'autres soutiennent que « métavers » n'est qu'un synonyme du cyberspace actuel, qu'il ne s'agit pas d'une nouveauté mais simplement de la réunion de

(1) Page « Get your business started in the metaverse » disponible à l'adresse : <https://www.facebook.com/business/metaverse>.

(2) Article « The metaverse explained: Everything you need to know » disponible à l'adresse : <https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know>.

(3) <https://secondlife.com/>.

(4) <https://www.minecraft.net>

(5) <https://www.meta.com/work/workrooms/>.

(6) Article « Zuckerberg says Meta and Apple are in 'very deep, philosophical competition' to build the metaverse » disponible à l'adresse : <https://www.theverge.com/2022/7/26/23279478/meta-apple-mark-zuckerberg-metaverse-competition>.

plusieurs technologies émergentes connexes. (7) Dès lors, on comprend qu'il n'existe pas encore de consensus sur ce qu'est ou n'est pas un métavers. Il peut impliquer le recours à des nouvelles technologies, comme des serveurs capables de gérer de nombreux utilisateurs en une seule instance ou des logiciels qui permettent de suivre les mouvements des yeux, bras ou jambes de l'utilisateur.

- L'avenir nous le dira, mais une chose est sûre : les métavers arrivent et, avec eux, une avalanche de questions sur le régime juridique des transactions, personnelles et commerciales, réalisées dans ces nouveaux mondes virtuels. Au premier rang de ces problématiques figure ce qui est sans doute le rituel juridique le plus important et le plus ancien : la signature de documents attestant de la convergence de vues entre les parties à un accord et de la formalisation d'un contrat.

Comment apposer sa signature électronique dans un métavers ?

- Une signature électronique est une donnée numérique jointe à un document transmis par voie électronique et qui prouve l'intention du signataire de signer ce document. Dans de nombreux pays, la signature électronique a la même valeur juridique que la signature manuscrite (du moins pour certaines transactions). Si de nombreuses organisations avaient déjà adopté la signature électronique pour gagner en sécurité et fiabilité, ce phénomène a pris encore plus d'ampleur depuis de la pandémie de coronavirus. (8)

- Cependant, on constate que beaucoup d'organisations utilisent les technologies qui leur tombent sous la main pour apposer ce qu'elles croient être des signatures électroniques fiables, sans tenir suffisamment compte de la sécurité ou d'autres aspects pratiques. Elles se heurteront au même écueil dans le métavers. Quelles seraient concrètement les modalités de signature dans un métavers ? On peut imaginer que des personnes participant, par le biais de leurs avatars, à une réunion dans une salle de conférence virtuelle, pourraient tout d'abord formuler leur consentement à un contrat oralement par le chat audio ou via le langage corporel de leurs avatars (hochement de tête, poignée de main). Cette étape peut être suivie de la transmission des versions électroniques des documents, de leur visualisation dans l'environnement simulé en tant qu'artefacts virtuels, et enfin de leur signature (pour ce faire, les participants peuvent taper leur nom ou faire un geste de signature manuscrite à l'aide d'un dispositif portable de suivi de mouvement qui reproduira la signature dans le métavers).

- À notre avis, rien n'interdit à un tribunal de considérer comme valable la signature de documents dans un métavers, pour autant que les parties aient respecté toutes les exigences applicables à la signature électronique en vertu de la loi du pays concerné, et qui sont généralement au nombre de trois : l'identité, l'intention et la force probante.

- Premièrement, l'identité : dans la grande majorité des cas, les signatures électroniques indiquent l'identité du signataire dans le cadre de communications électroniques. Dans le monde électronique, les systèmes identifient la plupart du temps les signataires au moyen d'identifiants uniques qui leur sont explicitement envoyés ou d'informations d'identification uniques. Un métavers peut conjuguer les deux, par exemple un identifiant unique sous la forme d'une URL spécifique ou

(7) Article « What Is the Metaverse, Exactly? » disponible à l'adresse : <https://www.wired.com/story/what-is-the-metaverse/>.

(8) Article « How to use electronic signatures securely » disponible à l'adresse : <https://www.michalsons.com/blog/how-to-use-electronic-signatures-securely/43260>

d'un PIN à usage unique transmis à l'utilisateur par courrier électronique ou par SMS, ou des informations d'identification uniques, comme un nom d'utilisateur et un mot de passe permettant à l'utilisateur de se connecter à la plateforme du métavers.

- Deuxièmement, pour constituer une preuve valable d'un accord, une signature électronique doit garantir son lien avec les données signées. Dans un métavers, elle matérialise l'acceptation par le signataire (par le truchement de son avatar) du contenu d'un message électronique en liant son identité avec ledit message auquel elle s'attache.

- Enfin, troisièmement, s'agissant de la force probante, les technologies associées à la signature électronique, telles que l'authentification multifactorielle (utilisée pour établir que le signataire est bien celui qu'il prétend être) et la cryptographie (servant à prouver qu'il a signé le document électronique en créant un artefact de preuve inviolable) peuvent clairement prouver l'identité et l'intention du signataire. Dans un métavers, la plateforme devra confirmer les étapes qui ont conduit à la signature, notamment la manière dont l'identité du signataire a été authentifiée, le moment où il a choisi d'apposer sa signature par le biais de son avatar ainsi que la manière suivie pour ce faire.

- Les signatures jouent donc un élément essentiel pour la vie commerciale dans la version actuelle du cyberspace, et il n'y a aucune raison pour qu'elles ne puissent pas continuer à jouer ce rôle dans le ou les métavers, sous réserve, bien entendu, que les parties à la transaction respectent toutes les exigences légales pertinentes.

Quels sont les risques associés à la signature électronique dans un métavers ?

- Dans le sillage de la pandémie de coronavirus, les tribunaux du monde entier vont être appelés à interpréter la validité de documents qui ont été signés électroniquement ou conclus par téléprésence.

- Prenons par exemple l'attestation de documents juridiques, tels que les affidavits. En effet, dans certains pays, la loi peut parfois exiger qu'une personne (le déclarant) soit assermentée par une autre spécialement habilitée à cette fin (le commissaire à l'assermentation) avant de signer un document afin de donner plus de force aux renseignements qu'il contient. Cette attestation doit se faire « *en présence* » du commissaire à l'assermentation. En principe, cette « *présence* » implique que le déclarant se présente physiquement, en personne, devant le commissaire à l'assermentation, prête serment et signe le document concerné.

- Certains pays, comme le Canada, se sont montrés progressistes et ont adopté une législation qui permet le recours à l'attestation à distance, et ont diffusés des conseils pour guider les parties dans la mise en œuvre de cette procédure.

- D'autres pays sont plus intransigeants. C'est le cas de l'Afrique du Sud, où un tribunal a pu reprocher à une partie d'avoir procédé à une attestation électronique de documents sans présence physique devant le commissaire à l'assermentation, avant de finalement accepter la validité de la procédure, au regard des circonstances de l'espèce et du respect de l'ensemble des autres exigences en matière d'attestation, non sans appeler au passage le législateur à mettre à jour

les dispositions obsolètes de la loi pour s’adapter aux pratiques commerciales actuelles dans le monde virtuel. (9)

▪ Qu’en serait-il si un tribunal sud-africain avait à connaître d’une attestation de document réalisée dans un métavers par les avatars virtuels du déposant et du commissaire à l’assermentation ? Le juge pourrait être tout aussi réticent à accepter que le document en question ait été valablement attesté, dressant ainsi un obstacle à l’utilisation de la signature électronique dans le monde virtuel. Sans une intervention du législateur, une telle décision de justice défavorable pourrait marquer un coup d’arrêt à la signature électronique dans le cyberspace, que ce soit dans notre version actuelle d’internet ou dans sa version future, composée d’un ou plusieurs métavers.

(9) Article « Firstrand Bank v Briedenhann, Virtual commissioning » disponible à l’adresse :

<https://www.michalsons.com/blog/firstrand-bank-v-briedenhann-virtual-commissioning/61105>

DAVID LUYT

south-africa@lexing.network



Metaverses and electronic signatures

▪ *Defining the concept of a metaverse is problematic because it is the coming together of several emerging technologies. It may be here already in some form or still coming as a possible successor to the Internet as we know it. Regardless, there is no reason that electronic signatures would not work in a metaverse – provided that the parties to the transaction comply with the requirements that they would have to abide ordinarily by for valid electronic signatures. We may have to reinterpret these slightly to account for signatories interacting through virtual avatars on metaverse platforms instead of with each other through our current signing software. However, suppose a court of a sufficiently high level takes a dim view of signatures in a metaverse because of having to interpret outdated legislation. In that case, it may derail the real possibility of electronic signatures in a metaverse. The moral of the story: lawmakers should update electronic transaction laws to allow for the precise and enforceable electronic signature of documents by electronic means. These electronic means could be through our current version of the Internet or a possible future one that we call some form or one or more metaverses.*

Why is it difficult to define a metaverse

- *Some people refer to ‘the Metaverse’ with a capital ‘M’, which usually means the upcoming product from Meta Platforms, Inc. (previously Facebook, Inc.) (1). We think it is more accurate to refer to ‘metaverses’ with a lowercase ‘m’ because we do not know what a metaverse is or how many of them there will be.*
- *A working definition of a metaverse might be a possible version of the Internet (or other smaller network) made up of a simulated world where virtual and augmented reality technologies allow people to participate as digital avatars. Various components could form a metaverse, including virtual enhancements to our physical reality (such as virtual reality headsets and gloves) and simulated spaces that continue to exist over time (such as conference rooms, social areas, or even whole worlds). (2)*
- *Metaverses arguably already exist in online video games with persistent worlds, such as Second Life (3) or Minecraft (4). A metaverse may also be the next version of conferencing software where people interact through virtual avatars instead of video chat, such as in Meta Horizon Workrooms (5). And one metaverse might win out over the others and become the future version of the Internet. (6)*
- *Some critics say that a metaverse is a synonym for our current cyberspace because it is not one new thing. Instead, it is the coming together of several related emerging technologies. (7) There are no hard-and-fast rules regarding what a metaverse is or is not. It may involve new technologies, such as servers that can handle many users in a single instance or motion-tracking software that detect where the user’s eyes are or where their limbs are in space.*

(1) See the web page titled ‘Get your business started in the metaverse’ available at: <https://www.facebook.com/business/metaverse>.

(2) See the article titled ‘The metaverse explained: Everything you need to know’ available at: <https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know>.

(3) See their website at: <https://secondlife.com/>.

(4) See their website at: <https://www.minecraft.net>

(5) See their website at: <https://www.meta.com/work/workrooms/>.

(6) See the article titled ‘Zuckerberg says Meta and Apple are in ‘very deep, philosophical competition’ to build the metaverse’ available at: <https://www.theverge.com/2022/7/26/23279478/meta-apple-mark-zuckerberg-metaverse-competition>.

(7) See the article titled ‘What Is the Metaverse, Exactly?’ available at: <https://www.wired.com/story/what-is-the-metaverse/>.

▪ Time will tell, but one thing is for sure – metaverses are coming, and with them, a slew of legal questions about how we govern our personal and business transactions in these brave new virtual worlds. Foremost amongst these is arguably the most significant and ancient legal ritual: the signing of documents to show a meeting of the minds between the parties to an agreement and the formalisation of a contract.

How might electronic signatures work in a metaverse?

▪ We generally understand electronic signatures as digital data attached to an electronically transmitted document that proves the signatory's intention to sign that document. They are the legal equivalent of handwritten signatures in many jurisdictions (at least for certain transactions). More and more organisations have been turning to electronic signatures to improve the security and reliability of their signing processes, and we have seen even greater adoption in the wake of the global coronavirus pandemic. (8)

▪ However, many organisations are using whatever technologies they can get their hands on to conclude what they believe to be reliable electronic signatures without sufficient consideration for security and other practical aspects. It is not hard to imagine how they would attempt to do so in a metaverse. For example, the parties to a meeting in a simulated conference room with virtual avatars may verbally agree to a contract through the audio chat features of that environment and then exhibit representations of acceptance through the body language of their avatars, such as the nodding of heads or the shaking of hands. They may then follow up this interaction by transmitting electronic versions of the documents to formalise their contract to each other, view them in the simulated environment as virtual artefacts and then purport to sign them by typing their names or making movements that apply their autographic signatures using their handheld motion-controlled devices.

▪ In our view, there is no reason why a court should not consider the parties to have signed these documents validly in a metaverse – provided that the parties complied with all relevant requirements for a valid electronic signature in that jurisdiction, which are usually: identity, intention, and evidential weight.

▪ When it comes to identity, electronic signatures indicate the identity of the signatory in the vast majority of instances of electronic communications. In the electronic world, systems typically identify signatories through unique identifiers explicitly sent to them or unique credentials. A metaverse may use both, such as a unique identifier in the form of a specific URL or one-time-PIN forwarded to the user by email or text message, or unique credentials, such as a username and password for the user to log into the metaverse platform.

▪ An electronic signature must be linked to the data intended to be signed for valid evidence of an agreement. In a metaverse, it must tell the story of how the user signing meant to agree to the contents of an electronic message through their avatar by tying their identity to it through an electronic signature.

▪ And turning to the issue of evidential weight, electronic signatures have a greater capacity to positively prove identity and intent by using technologies, such as multi-factor authentication, to establish that the signatory is who they claim to be and

(8) See our article titled: 'How to use electronic signatures securely' available at: <https://www.michalsons.com/blog/how-to-use-electronic-signatures-securely/43260>

cryptography to prove that they signed the electronic record by creating a tamper-proof evidentiary artefact. In a metaverse, the platform would need to confirm the steps that lead up to the signature – such as how the signatories' identity was authenticated and when and how they chose to apply their signature through their avatar.

- Signatures are a critical part of our commercial lives, and there is no reason why they could not continue to be so through a metaverse as they currently are through the current iteration of cyberspace, provided that the parties to the transaction comply with all relevant legal requirements.

What could go wrong with electronic signatures in a metaverse?

- Courts worldwide are being called upon to interpret the validity of documents signed electronically or otherwise concluded via telepresence in the wake of the coronavirus pandemic.

- Take the phenomenon of commissioning legal documents, such as affidavits, for example. In the physical world, commissioning documents typically involves the deponent appearing in the physical presence of the commissioner, taking an oath and signing the document concerned.

- In the electronic world, some jurisdictions (such as Canada) have been progressive and brought in legislation that allows for electronic commissioning and guidance explaining how to commission documents electronically.

- Others have been less progressive, such as South Africa, where the courts have been critical of people not taking steps to comply with the physical presence commissioning requirements in outdated laws (although they subtly called upon the lawmakers to update those laws) and begrudgingly accepted electronically commissioned documents because the parties complied with the substance of all requirements. (9)

- Suppose a South African court were to consider the phenomenon of a commissioner of oaths commissioning a document in a metaverse through their virtual avatar interacting with the deponent through their virtual avatar. In that case, the court might be similarly reluctant to accept that the document in question was validly commissioned. This kind of decision could derail the process of validly signing documents in a metaverse unless lawmakers take steps to address these issues in cyberspace – whether our current iteration of the Internet or a hypothetical future version that may involve one or more metaverses.

(9) See the article on our website titled 'Firststrand Bank v Briedenhann | Virtual commissioning' available at: <https://www.michalsons.com/blog/firststrand-bank-v-briedenhann-virtual-commissioning/61105>

DAVID LUYT

south-africa@lexing.network



Métavers et vie privée

Nouveau monde, nouvelles règles ? Parallèles entre la vie privée dans le domaine physique et dans le domaine numérique

▪ Avec le métavers, nous approchons la nouvelle frontière d'Internet, et la question que nous devrions nous poser est « *sommes-nous prêts ?* ». Aujourd'hui, la puissance calcul colossale disponible, l'intelligence artificielle et l'internet des objets ouvrent le champ de possibles dans les mondes physique et numérique. Les individus peuvent désormais se connecter les uns aux autres dans un monde virtuel simulé grâce aux technologies de la réalité virtuelle (RV), de la réalité augmentée (RA) et de la blockchain. Si des jeux comme Roblox, Fortnite et Minecraft ont fait connaître au grand public le concept de métavers, les investissements réalisés dans le métavers par les GAFAM (Microsoft, Meta etc.) indiquent bien que ce nouveau monde offre, au-delà de ses aspects ludiques, de réelles opportunités commerciales. Dans ce contexte d'effervescence, les autorités de protection des données et de la vie privée ont bien du mal à suivre le rythme effréné auquel évoluent les technologies .

Comment la législation en matière de protection de la vie privée existant en Australie et à l'étranger s'appliquera à ce nouveau monde ?

- Collecte, utilisation et divulgation de données personnelles

▪ Poussée par des récentes violations de données très médiatisées affectant l'opérateur téléphonique Optus et l'assureur santé Medibank Private, l'Australie s'apprête à introduire une série de réformes en matière de protection de la vie privée. De manière générale, le régulateur australien s'intéresse de plus en plus aux aspects numériques et notamment à l'utilisation de données biométriques via les technologies d'intelligence artificielle (IA).

▪ Pour interagir dans le monde virtuel, les utilisateurs se munissent d'équipements de réalité virtuelle. Or, ces équipements collectent souvent bien d'autres données que celles nécessaires à la transmission des mouvements de l'utilisateur dans un jeu ou un monde virtuel : ils peuvent, en effet, également recueillir des informations biométriques (démarche, mouvement des yeux, réponse physiologique de l'utilisateur). En Australie, ces données bénéficient d'une protection renforcée car elles sont considérées comme des données sensibles en vertu de la loi de 1998 sur la protection de la vie privée (*Privacy Act 1988 (Cth)*) et leur collecte et leur utilisation sont donc soumises à des règles plus strictes. Par exemple, dans de nombreux cas, les données biométriques ne peuvent être collectées qu'avec le consentement exprès de l'utilisateur et que si ces données sont raisonnablement nécessaires pour une des activités poursuivies par le responsable du traitement.

▪ Le type et le volume des données collectées dans le métavers rendent possibles des nouvelles formes sophistiquées de marketing. La question essentielle qui s'impose d'emblée est de savoir si, compte tenu de la vitesse et de la fluidité de la collecte et des échanges de données dans ce monde virtuel, les entreprises

pourront s'acquitter, dans le métavers, des obligations qui leur incombent actuellement en matière de respect de la vie privée et de la protection des données dans le « monde réel », ou si ce cadre juridique devra être entièrement repensé pour s'appliquer au métavers.

- Le cadre juridique de protection de la vie privée et de la protection des données personnelles dans le métavers

- L'un des principaux objectifs du métavers est de mettre en place un monde numérique intégré et interopérable. Cela suppose que les données collectées par une entreprise dans le métavers puissent circuler de manière transparente entre les différents opérateurs et les différentes plateformes pour permettre, par exemple, à un utilisateur d'acheter un actif numérique sur une plateforme et de l'utiliser ou de le vendre sur une autre. Pour que cela soit possible, non seulement les entreprises devront conclure des contrats de partage des données, mais les législateurs auront aussi à mettre en place un système mondial robuste permettant une application cohérente et harmonisée des lois internationales sur la protection de la vie privée. En Australie, en vertu de la loi sur la protection de la vie privée, les entreprises ne peuvent transférer des données personnelles à un destinataire étranger que sous réserve du respect des principes australiens de protection de la vie privée et elles demeurent en outre pleinement responsables en cas d'utilisation abusive.

- De même, en Europe, le règlement général sur la protection des données (RGPD) n'autorise les transferts de données à caractère personnel concernant les citoyens et résidents de l'UE vers des pays tiers que si le pays destinataire est considéré comme assurant un niveau adéquat de protection des données. Ces règles instaurées par le *Privacy Act* australien et le RGPD européen ne sont pas forcément compatibles avec la nature mondiale et transversale du métavers. Pour ajouter à la complexité, la tendance mondiale actuelle tend vers l'imposition de la localisation des données sur le territoire national et l'application de restrictions croissantes concernant leur sortie du pays où elles ont été collectées.

Prochaines étapes

- Pour conclure, et pour répondre à la question initialement posée, force est de constater que, pour l'instant, nous ne sommes pas encore prêts pour le métavers, du moins du point de vue de la protection des données et de la vie privée. Toutefois, de la même manière que l'avènement des réseaux sociaux il y a presque vingt ans a entraîné des changements législatifs, il y a fort à parier que les autorités vont s'adapter au fur et à mesure de la popularisation du métavers.

DUDLEY KNELLER

[australia@
lexing.network](mailto:australia@lexing.network)



Metaverse and privacy

New world, new rules? The parallels of privacy between the physical and digital realms

▪ *The world is entering the next internet frontier, and the question we should be asking is "are we ready for it?" Unprecedented processing power, artificial intelligence and the 'Internet of Things' presents limitless possibilities in both the physical and digital environment. Individuals can now connect with each other in a simulated virtual world thanks to AR, VR and block chain technology. While games like Roblox, Fortnite and Minecraft have brought the concept of the metaverse to the mainstream, investments in the metaverse by tech giants like Microsoft and Meta indicates this new world offers commercial opportunities too. Amidst the buzz and excitement of what the metaverse can offer, privacy regulators are struggling to keep up.*

How will existing Australian and overseas privacy principles apply in this new world?

- *Collection, use and disclosure of personal information*

▪ *Australia is again on the verge of introducing a raft of privacy reforms following well publicised data breaches affecting Optus and health insurer, Medibank Private. The regulator has already focussed its attention on the use of biometric data by AI technologies and is taking an increasing interest in all things digital in Australia.*

▪ *The metaverse relies on the use of VR equipment for users to interact in the virtual world, which often is capable of collecting data beyond transmitting the user's movement in a game or virtual world. It can also collect biometric information like the user's gait, eye movement and physiological response, which is considered sensitive information under Australia's Privacy Act 1998 (Cth) (Privacy Act) and attracts greater protections relating to its collection and use. In many cases, biometric information must not be collected without the express consent of the user and only if that information is reasonably necessary for one or more of the organisation's functions and activities.*

▪ *The type and volume of the data collected simply by participation in the metaverse will enable new, sophisticated forms of marketing to be integrated in the digital world. The key question in this case would be whether businesses can discharge their privacy obligations currently required in the "real world" in the same way in the metaverse where data is collected and exchanged at such a high speed, frictionless level, or whether a privacy framework for the metaverse will need to be workshopped altogether.*

- *The privacy framework in the metaverse*

▪ *One of the key intentions for the metaverse is how integrated and interoperable the digital world could be. Data collected by one company in the metaverse should*

be able to seamlessly flow between various operators and platforms to allow, for example, a user to buy a digital asset in one platform and use or sell it in another. Enabling this would require companies to not only implement data sharing agreements, but would also require a robust, global system to allow international privacy laws to operate with each other. Under Australia's Privacy Act, companies must handle personal information of an overseas recipient in accordance with the Australian Privacy Principles and remain accountable for that person's data in the event the information is mishandled.

- *For data concerning EU citizens and residents, the General Data Protection Regulation (GDPR) only permits data transfers to non-EU countries if the receiving country is considered to have an adequate level of personal data protection. However, our traditional understanding of data locality under privacy regimes like the Australian Privacy Act and the GDPR is not entirely congruent with the worldwide, transcendent nature of the metaverse. This is especially complicated by a global trend towards data localisation and increasing restrictions for data leaving the country where it was collected.*

So what's next?

- *From a privacy standpoint, the answer to whether we are ready for the metaverse would be "no, not really". But in the same way we saw the advent of social media two decades ago drive legislative change, we are also likely to see regulators respond similarly as more and more individuals and organisations take advantage of the opportunities the metaverse presents.*

DUDLEY KNELLER

[australia@
lexing.network](mailto:australia@lexing.network)



Métavers et propriété intellectuelle : la propriété intellectuelle doit-elle être transnationale ?

- Le métavers est un espace virtuel, collectif et partagé de réalité augmentée rassemblant les humains dans un monde numérique.
- Pour l'instant, l'univers du jeu est majoritairement présent dans cette réalité numérique immersive. Pour preuve, alors qu'on estime que d'ici 2026, cet écosystème comptera 2 milliards de participants **(1)**, un joueur brésilien sur dix a déjà, directement ou indirectement, expérimenté le métavers **(2)**.
- Le métavers cristallise aujourd'hui l'attention et de nombreuses études se penchent sur les différentes facettes de ce phénomène, que ce soit sous l'angle humain, par exemple pour analyser les relations humaines qui y sont intrinsèquement présentes, ou sous l'angle juridique, afin de déterminer le droit applicable et notamment le régime de protection de la propriété intellectuelle.
- En effet, comment protéger les droits d'auteur, les logiciels, les technologies ou encore les marques et les brevets dans le métavers ? Il s'agit là de questions essentielles qui doivent soulevées et appréhendées au moment où le métavers est encore en pleine construction.
- Récemment, Hermès, l'une des plus grandes marques du secteur de la mode, s'est retrouvée confrontée à la mise en vente dans le métavers, sur la plateforme OpenSea, d'un sac dénommé « MetaBirkin » reproduisant à l'identique son sac emblématique « Birkin » **(3)**. Cette création numérique pouvait être source de confusion auprès des consommateurs et faire croire à une association avec Hermès, ce qui n'était pas le cas puisque le « MetaBirkin », créé par un artiste indépendant, n'avait rien à voir avec le géant de la mode. Hermès a décidé de porter l'affaire en justice.
- Dans ce genre de cas, quelles sont justement les lois applicables et les tribunaux compétents pour ce qui concerne le métavers ? Les paramètres judiciaires actuels sont-ils limités à l'analyse comparative entre produits réels et produits numériques ? La similitude des caractéristiques entre des produits et services composés dans des environnements différents compromet-elle le brevet créé ou la marque exploitée ? Il est en tout état de cause recommandé aux entreprises de procéder aux enregistrements appropriés dans tous les pays dans lesquels elles ont l'intention de se projeter dans le métavers.
- Sachant qu'un brevet, une marque ou un logiciel peuvent avoir des propriétaires différents dans différents pays, les multinationales vont devoir élaborer une stratégie prenant en compte ce monde virtuel pour assurer la protection de leurs actifs de propriété intellectuelle (brevets, marques, etc.) dans le métavers.
- La propriété intellectuelle repose sur des droits territoriaux, mais le métavers, par nature décentralisé, crée un monde sans frontières, et lui confère un nouvel aspect transnational.

(1) <https://exame.com/future-of-money/pesquisa-afirma-que-2-bilhoes-de-pessoas-estarao-no-metaverso-ate-2026/>

(2) <https://noomis.febraban.org.br/blog/um-em-cada-10-gamers-brasileiros-ja-entrou-no-metaverso-diz-pesquisa>

(3) <https://glamurama.uol.com.br/moda-e-design/hermes-processa-artistas-que-criaram-versao-da-bolsa-birkin-para-o-metaverso/>

▪ Au Brésil, les brevets, marques et autres créations industrielles (dessins et modèles) sont protégés par la loi n°9.279/96 (loi sur la propriété industrielle) qui en garantit l'utilisation, la jouissance et la propriété. Cette loi spécifie les procédures de délivrance et d'enregistrement pour chaque type d'invention auprès de l'INPI, l'institut national de la propriété industrielle, (*Instituto Nacional da Propriedade Industrial*), ainsi que les mesures mises en place pour combattre les atteintes portées aux droits associés et lutter contre la concurrence déloyale (4).

(4)
http://www.planalto.gov.br/ccivil_03/leis/l9279.htm

▪ Toutefois, la législation brésilienne ne paraît plus suffisante pour faire face à l'élargissement du domaine des marques provoqué par les médias numériques et une base juridique plus solide est donc nécessaire pour offrir davantage de sécurité aux acteurs économiques dans cet « univers sans frontières » qu'est le métavers.

▪ Conformément à la loi, les marques et les brevets doivent être exploités pour bénéficier du maintien en vigueur de leur protection. Dès lors, tout l'enjeu est de concevoir un cadre applicable à ces multiples innovations qui transcendent les frontières et forment un environnement universel.

▪ En 2018, le Brésil a accepté le protocole portant amendement de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (« Accord sur les ADPIC »), adopté par le Conseil général de l'Organisation mondiale du commerce le 6 décembre 2005 (5). Cet amendement, qui s'applique à la commercialisation internationale de produits pharmaceutiques, peut être transposé, par analogie, à d'autres marchés qui deviennent transnationaux, comme le marché du numérique.

(5)
http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/decreto/D9289.htm

▪ Plus récemment, en 2019, l'entrée en vigueur au Brésil du Protocole de Madrid, a élargi les compétences et les pouvoirs de l'INPI brésilien (6). Les missions de l'INPI s'articulent désormais autour de deux activités principales, d'un côté l'enregistrement national de brevets, marques et inventions, et de l'autre, la gestion des demandes internationales déposées par des utilisateurs étrangers.

(6)
<https://www.gov.br/inpi/pt-br/servicos/marcas/protocolo-de-madri>

▪ Ces accords, protocoles et législations renforcent la sécurité des titres de propriété intellectuelle.

▪ Ce contexte semble de bon augure au vu du développement du métavers. Reste à voir s'il sera suffisant en fonction des effets que le métavers pourrait concrètement induire à l'avenir.

ANDREA FILOMENO
&
GUILHERME
GUIMARÃES VIEIRA

brazil@lexing.network



**Metaverse and Intellectual Property:
Should Intellectual Property be transnational?**

- *The metaverse by definition is considered a collective virtual shared and augmented reality space that aims to integrate different components of the digital world with humans.*
- *According to several surveys, one in every 10 Brazilian gamers has already entered the metaverse or experienced it in some manner (1). Another interesting statistic estimates that by 2026 this ecosystem will have 2 billion participants (2). It is easy to conclude, therefore, that the gaming universe is increasingly present in the immersive digital reality.*
- *There has been a significant increase in the search for explanations about the theme, that is, the metaverse has attracted a lot of attention. Taking into account that the human relationship is intrinsically present in the metaverse, that is, the law is applicable to the platform in question, and the reach of the global legal market gains traction in the protection of intellectual property in this metaverse ecosystem.*
- *The copyrights, the types of software, the technology involved, and the exploited brand are mechanisms and factors that demand legal protection in regards to their treatment within the metaverse. Accordingly, the normative universe, through intellectual property, has ramifications that deserve to be observed during the construction of the metaverse for the due fulfillment of patent and trademark registrations.*
- *Recently, Hermés, considered one of the most notable brands in the fashion world, found itself under pressure after the identical use of its "Birkin" bag - a female icon - being sold on OpenSea, a metaverse platform, under the name "MetaBirkin" (3). The creation of the digital collection had repercussions, as it could generate some consumer confusion and association with Hermés. The "MetaBirkin", however, was created by an independent artist and had nothing to do with the fashion giant. In this case, Hermés had no choice but to initiate a legal battle.*
- *Given this fact, which jurisdictions are applicable to the metaverse? Are the current judicial parameters restricted to the comparative analysis between real and digital products? Does the similarity of characteristics between products and services composed in different environments compromise the patent created or the trademark exploited? It is recommended, indeed, that companies have the proper registrations in all jurisdictions in which they intend to project themselves in the metaverse.*
- *It is known that the same patent, trademark or software may have different owners in different countries. It can be seen, therefore, that multinational*

(1) <https://noomis.febraban.org.br/blog/um-em-cada-10-gamers-brasileiros-ja-entrou-no-metaverso-diz-pesquisa>

(2) <https://exame.com/future-of-money/pesquisa-afirma-que-2-bilhoes-de-pessoas-estarao-no-metaverso-ate-2026/>

(3) <https://glamurama.uol.com.br/moda-e-design/hermes-processa-artistas-que-criaram-versao-da-bolsa-birkin-para-o-metaverso/>

organizations will have to work hard at developing a patent, trademark and product strategy in the metaverse.

- Intellectual property is based on territorial rights, but with the rise of the metaverse, represented by decentralization, creating a world without borders, intellectual property gains new transnational aspects of spatial occupation.

- In Brazil, Law n^o. 9.279/96 (Industrial Property Law) provides regulatory instruments to protect and ensure the use, enjoyment, and ownership of a patent, trademark, or industrial creation (design). In this law, one can verify registration procedures, specific protocol forms for each type of invention, and measures to combat the improper use of registrations granted by the INPI (National Institute of Industrial Property), seeking to repress unfair competition **(4)**.

- In this aspect, the Brazilian legislation is no longer sufficient for the brand enlargement caused by digital media. That is, the market needs more legal grounding to offer security to market agents in this “borderless universe” that is the metaverse.

- Trademark and patent rights must be enforced to protect their use in accordance with the law. The challenge, however, is to design a framework that is applicable to so many innovations that transcend the boundaries of nations, resulting in a universal environment.

- Thus, in 2018, Brazil joined and enacted the Protocol of Amendment to the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement"), adopted by the General Council of the World Trade Organization on December 6, 2005 **(5)**. This agreement aims to regulate the international commercialization of the pharmaceutical sector, but it can be used analogously, through interpretation, in other markets that become transnational, extracting the basis for other sectors, such as the digital one.

- More recently, in 2019, the Madrid Protocol came into force in Brazil, offering the INPI new horizons and new realms of activity **(6)**. In this case, the INPI began to develop two core activities, the first being to act as an internal and national base for the registration of patents, trademarks and inventions with international guarantee, and, the second, as a designated office to receive international applications from foreign users.

- That said, with this legal mesh offered by agreements, protocols, and local legislation that can be communicated around the world, new possibilities are provided for ensuring security in the face of interchangeable and international records.

- This legal scenario seems promising for the metaverse trends proposed by digital programmers. It remains to be seen what practical effects the use of metaverse will bring to the new generations.

(4)

http://www.planalto.gov.br/ccivil_03/leis/l9279.htm

(5)

http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/decreto/D9289.htm

(6)

<https://www.gov.br/inpi/pt-br/servicos/marcas/protocolo-de-madri>

ANDREA FILOMENO
&
GUILHERME
GUIMARÃES VIEIRA

brazil@lexing.network



L'identité numérique dans le(s) métavers

- L'identité numérique est une question cruciale pour le(s) métavers. Il est en effet essentiel de définir clairement comment les personnes se connecteront au(x) métavers et y évolueront sous couvert d'un avatar. L'enjeu est bien évidemment de garantir et de sécuriser cette identité pour créer la confiance nécessaire aux interactions dans ce nouveau monde. Les questions pleuvent : comment vérifier qu'une personne est bien celle qu'elle prétend être ? Une même personne peut-elle utiliser différents avatars ? Son identité est-elle interopérable dans les différents métavers ? Son identité réelle doit-elle être forcément divulguée ou un certain anonymat pourra-t-il être conservé en fonction du type d'interaction ?
- En Espagne, la Charte des droits numériques érige l'identité numérique en un droit, y compris dans des environnements tels que le métavers, et confère notamment le droit de la gérer pleinement, avec tous ses attributs. Ce texte, même en l'absence de caractère normatif, constitue un cadre de référence et son application nécessite l'établissement de garanties pour permettre la vérification sécurisée de l'identité dans le métavers afin d'éviter la manipulation, l'usurpation ou le contrôle de son identité numérique par des tiers non autorisés.
- Récemment, Europol **(1)** a publié un rapport dans lequel cette agence européenne spécialisée dans la répression de la criminalité insiste sur les nombreuses menaces qui planent sur l'identité numérique dans le métavers. La quantité et le niveau de détail des informations disponibles dans le métavers offrent aux cybercriminels la possibilité de créer des « identités synthétiques », c'est-à-dire des identités qui mêlent vrais et fausses informations à des fins frauduleuses. Cette technique peut se combiner aux hypertrucages, plus connus sous le terme anglais *deepfakes*, qui, grâce à l'utilisation de l'intelligence artificielle (IA), permettent de modifier les traits du visage d'une personne ou le son de sa voix de manière très réaliste. On pense au *deepfake* de l'acteur Tom Cruise diffusé sur le réseau TikTok ou encore à celui mettant en scène l'ex-président américain Barack Obama dans lequel on le faisait tenir des propos insultants envers ses rivaux politiques. Si ces vidéos truquées, devenues virales, avaient un but parodique, on imagine bien qu'elles peuvent ouvrir la voie aux usurpations d'identité en tout genre lorsqu'elles sont utilisées pour tromper et manipuler les internautes à des fins criminelles. C'est dans cette optique que la proposition de règlement européen sur l'IA **(2)** prévoit notamment d'imposer des obligations de transparence aux systèmes d'IA utilisés pour générer ou manipuler des images ou des contenus audio ou vidéo présentant une ressemblance avec des personnes existantes et pouvant être perçus à tort comme authentiques ou véridiques.
- L'identité numérique souveraine (identité auto-souveraine ou SSI), qui garantit à l'utilisateur la propriété de ses données personnelles et le pouvoir de contrôler la façon dont ses données sont partagées et utilisées, est une des solutions possibles aux problèmes d'identité dans le métavers, en particulier pour les métavers décentralisés tels que Decentraland et The Sandbox, qui reposent sur la technologie de la *blockchain* et les jetons non fongibles (NFT).

(1) Europol (2022) Le maintien de l'ordre dans le métavers : ce que les services répressifs doivent savoir <https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know>

(2) Article 52 Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union : COM(2021) 206 final

MARC GALLARDO

[spain](#)
[@lexing.network](#)



Digital identity in the Metaverses

- *One of the key legal issues is how people will connect to the Metaverse or Metaverses and how they will identify themselves to have sufficient legal certainty in their interactions, through their avatars. How to know that someone is who they say they are? Can the same person use different avatars and that their identity is interoperable in the Metaverses? Can their identity be known, or may sufficient identification be required depending on each type of interaction?*
- *The Digital Rights Charter in Spain elevates one's own digital identity to the category of enforceable right in environments such as the Metaverse or Metaverses, including the right to manage and accredit it fully, with all its attributes. The proclamation of this right, even with a programmatic and non-normative character, requires the establishment of necessary guarantees that allow the secure verification of the identity in the Metaverses in order to avoid manipulation, impersonation or control of the digital identity by unauthorized third parties.*
- *Recently, Europol (1) has analyzed how digital identities are one of the most important assets in the Metaverses, and how they are threatened through very diverse acts of impersonation, which allow to generate synthetic identities with a high level of detail of a person performing actions on their behalf. Think of the deepfakes that, through the use of editing software with Artificial Intelligence (AI) systems, allows you to manipulate the facial features of a person in a very realistic way, in addition to synthesizing their voice, and therefore fertilize the ground for impersonations of all kinds, including not only parodies such as the deepfake of Tom Cruise in an account of the social network TikTok or that of Barack Obama insulting his political rivals, but those carried out for criminal purposes. In this regard, it should be noted that the Proposal for a European Artificial Intelligence Act (2) provides for transparency obligations for AI systems designed to act with people; so that users who generate or manipulate image, sound or video content that significantly resembles people and that may erroneously lead to think that they are authentic, must make public that the content has been artificially generated.*
- *The sovereign digital identity (self-sovereign identity or SSI), understood as the digital identity model in which the users are the owners of their personal data and have the power to control how their data are shared and used, is one of the solutions presented to face this legal challenge, especially for decentralized Metaverses such as Decentraland and the Sandbox, among others, based on blockchain technology and non-fungible tokens (NFTs).*

(1) Europol (2022) Policing in the metaverse: what law enforcement needs to know <https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know>

(2) Article 52 of the Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts: COM/2021/206 final

MARC GALLARDO

[spain](#)
[@lexing.network](#)



Métavers et médecine :

le métavers médical, un outil clinique de formation, de test et de traitement

- Alors que nous ne sommes qu'à l'aube du métavers, son utilisation dans le secteur de la santé est déjà en pleine expansion grâce aux progrès techniques, boostés par le rôle majeur joué par la télémédecine pendant la pandémie de coronavirus.
- La réalité virtuelle (RV) et la réalité augmentée (RA) sont d'ores et déjà utilisées à des fins médicales, d'une part, pour tester et traiter des patients confrontés à différents troubles cognitifs, psychologiques et moteurs et, d'autre part, pour former et entraîner des médecins. Des patients humains virtuels (VH) ont ainsi été créés pour accompagner la formation des étudiants en médecine aux techniques de chirurgie cardiaque ou celles des enquêteurs cliniques à l'analyse du comportement des patients nécessaire pour déterminer leur l'état psychologique. Les médecins s'entraînent à observer les expressions faciales, les gestes et la voix du patient virtuel afin de procéder à des évaluations cognitives. Avec l'aide de la RV et de la RA, de nouvelles méthodes de recherche et d'essais cliniques sont également développées.
- Le métavers fait, en plus, tomber les barrières entourant le traitement clinique des patients. Par exemple, des moniteurs de pression sanguine, de fréquence cardiaque et de saturation en oxygène peuvent être directement intégrés dans le métavers, ou encore des personnes paralysées sont capables, une fois équipées de casques de RV, d'y suivre une thérapie physique virtuelle. Le groupe Thumbay, basé à Dubaï, va lancer le premier hôpital au monde existant uniquement dans le métavers. Cet hôpital virtuel intègrera une université de médecine et un espace dédié au bien-être virtuel. La société Aimesis Avalon, présente aux Pays-Bas et aux Émirats arabes unis, n'est pas en reste et se félicite, pour sa part, d'être le plus grand espace de soins de santé du métavers **(1)**.
- Autre domaine médical de prédilection dans le métavers : le traitement clinique de la santé mentale. Les plateformes de métavers, telles que Decentraland, sont des lieux d'interaction entre utilisateurs, et constituent potentiellement un vecteur de soutien social aux patients. A l'aide des casques de VR et d'ordinateurs portables standard, les patients souffrant d'anxiété, d'autisme, de toxicomanie et de traumatismes divers rejoignent, via leurs avatars virtuels, des plateformes de chat interactives pour participer à une thérapie individuelle ou de groupe **(2)**. Cette démarche s'inscrit dans la logique de thérapies immersives similaires, quoique plus intensives, mises en place auprès de groupes de réfugiés rwandais exposés à des traumatismes importants via la thérapie d'exposition narrative **(3)**, ou auprès d'enfants atteints d'autisme **(4)** ou de traumatismes liés aux abus sexuels via la thérapie par le jeu de sable **(5)**.
- A un niveau plus avancé, il existe la thérapie par exposition à la réalité virtuelle (*Virtual Reality Exposure Therapy*, ou VRET) pour traiter les formes sévères de syndrome de stress post-traumatique (aussi connu sous son acronyme anglais

(1) <https://thumbay.com/business-sectors/healthcare>

(2) <https://aimedis.io/metaverseRizzo, A. & Shilling, R., Clinical Virtual Reality tools to advance the prevention, assessment, and treatment. Eur J Psychotraumatol. Publié en ligne le 16 01 2017 https://pubmed.ncbi.nlm.nih.gov/29372007/>

(3) Jacob, N. Neuner, F., Maedl, A., Schaal, S., & Elbert, (2014) Dissemination of psychotherapy for trauma spectrum disorders in postconflict settings: A randomized controlled trial in Rwanda. *Psychotherapy and psychosomatics*, 83 (6), 354-363.

(4) Iran J Public Health. 2021 Oct;50(10):2046-2054. doi: 10.18502/ijph.v50i10.7505. Effects of Image-Sandplay Therapy on the Mental Health and Subjective Well-Being of Children with Autism; [Juan Guo](#), [Dongmei Li](#), Affiliations expand PMID: 35223572 PMCID: [PMC8819219](#) DOI: [10.18502/ijph.v50i10.7505](#)

(5) *Frontiers in Psychology*. 2017 May 4;8:617. doi: 10.3389/fpsyg.2017.00617. eCollection 2017. Change during Psychotherapy through Sand Play Tray in Children That Have Been Sexually Abused, [María D L Angeles Tornero](#), [Claudia Capella](#)

PTSD) résultant de traumatismes et d'agressions sexuelles. Cette approche thérapeutique intensive fondée sur des données probantes, appelée BRAVEMIND, a été développée par l'Institut pour les technologies créatives de l'Université de Californie du Sud (USC-ICT), en partenariat avec le gouvernement américain, afin d'aider les soldats revenant d'Irak et d'Afghanistan. Muni d'un casque de RV, l'utilisateur se retrouve immergé dans une situation virtuelle et reçoit des stimuli visuels, auditifs (son 3D directionnel), tactiles (vibrations) et olfactifs (odeurs). Plutôt que de s'en remettre exclusivement à son imagination pour se mettre en situation, avec BRAVEMIND, le vétéran revit son traumatisme de manière immersive dans le monde virtuel mais dans un espace encadré et sécurisé. Le stimulus est en effet supervisé par le médecin via une interface séparée et le professionnel de santé garde en permanence un contact audio avec son patient.

- Le programme BRAVEMIND de l'USC-ICT, initialement limité à la sphère militaire, a fait ses preuves au point d'être ensuite étendu à la population civile. Actuellement, ce système est déployé aux États-Unis dans plus de 60 sites (6), au Canada et en Norvège et fait l'objet d'études cliniques au Brésil visant à évaluer tester l'efficacité de la VRET comme traitement d'appoint pour les patients souffrant de crises de panique (7). Tout ceci laisse penser que les applications cliniques de la RV sont appelées à devenir des outils indispensables pour les psychologues et les médecins et vont gagner en popularité.

- Que faudra-t-il pour que le métavers médical soit adopté par tous ? L'argent est naturellement le nerf de la guerre : une injection massive de capitaux est essentielle pour faire progresser la technologie. Dans cette optique, les fabricants de dispositifs médicaux s'associent à des développeurs de RV. A titre d'exemple, le fabricant de dispositifs de chirurgie de la colonne vertébrale Spineology, a fait appel à Ghost Productions, un développeur de simulations chirurgicales de RV, en vue de dispenser à ses équipes de vente une formation intégrant la RV. Le but : familiariser les commerciaux avec ses produits pour qu'ils puissent mieux les vanter auprès des prospects (8). En ce qui concerne la RA, les entreprises jouent des coudes pour s'imposer dans ce secteur. Aris MD propose des visualisations 3D de l'anatomie du patient, sur lesquelles le chirurgien s'appuie pour effectuer la procédure dans un espace virtuel. Echopixel, quant à elle, crée un « jumeau numérique » du patient à partir d'images médicales standard, fournissant ainsi aux médecins un « hologramme 4D interactif ».

- Mais au-delà l'aspect financier, le succès du métavers médical dépendra également de la gestion des questions liées à la protection de la vie privée des patients. Si les principes de réalité virtuelle et de télémédecine sont des pierres angulaires, aux États-Unis par exemple, des lois supplémentaires sont nécessaires pour garantir la confidentialité et la protection des données des patients.

- A défaut pour le législateur américain d'adopter un cadre complet de lois fédérales sur la vie privée et la cybercriminalité, la généralisation du métavers médical devra donc nécessairement passer par l'utilisation de nouvelles technologies, telles que celles permettant des restrictions des accès ou encore la blockchain.

(6) <https://ict.usc.edu/research/projects/bravemind-virtual-reality-exposure-therapy/>

(7) Faria, C., Santos, V., Muniz, M., Do Cabo, M., Nardi, A., & Da Rocha Freire, R. (2021). Virtual reality exposure therapy in panic disorder: A pilot study. *BJPsych Open*, 7(S1), S251-S251. doi:10.1192/bjo.2021.672

(8) Are metaverse applications becoming a reality in medical training? 24 08 2022 <https://www.metaverselearningspace.com/are-metaverse-applications-becoming-a-reality-in-medical-training/>

JANICE F. MULLIGAN

usa@lexing.network



**Metaverse and Medicine:
Medical Metaverse as a Clinical Tool to Train, Test and Treat**

- While it is just the dawn of the metaverse, the sun is quickly rising on the use of the metaverse in health care. This is possible due to technical advancements in technology, coupled with the wildly successful proliferation of telemedicine during the pandemic.
- Both virtual reality (VR) and augmented reality (AR) are being used for training and teaching doctors, as well as testing and treating patients for a variety of cognitive, psychological, and motor disorders. Virtual human patients (VH) have been developed for such varied uses as training student surgeons in procedural cardiac surgery techniques and teaching clinical interviewers how to perform behavior analysis to determine patients' psychological condition. Doctors are also being trained to analyze the VH's facial expressions, gestures, and voice to make cognitive assessments. New ways of doing research and conducting clinical trials are also being developed with the assistance of VR and AR.
- The metaverse is also being used to break down barriers for clinical patient treatment. Blood pressure, heart and oxygen saturation monitors, are all being directly integrated inside the metaverse. VR headsets are also being used to help people with paralysis, by assisting with intense ongoing virtual physical therapy. The Dubai-based Thumbay Group, is launching the world's first completely metaverse hospital, which includes a metaverse medical university and a virtual wellness domain. Also leading the pack is the Netherlands and UAE based company Aimeidis Avalon, which promotes itself as the biggest healthcare space in the metaverse (1).
- The most robust medical development is the use of the metaverse for clinical mental health treatment. At a basic level, the metaverse enables social support for patients by using platforms which enable user interaction similar to the initial metaverse virtual worlds of Decentraland (and other similar platforms.) Low-cost VR headsets and laptops allow patients to immerse their virtual human avatars into interactive chat-room platforms where both individual and group therapy are offered to patients suffering from anxiety, autism, substance abuse and trauma (2). Similar but more intensive immersive therapy have been used with Rwandan refugee groups who had significant trauma exposure (3). Additionally, children are being treated for autism (4) and trauma from sexual abuse with Virtual Sandtray for children's narrative play therapy (5).
- A more advanced direct virtual reality exposure therapy (VRET) is also used to treat severe Post-Traumatic Stress Disorder (PTSD) arising from trauma and sexual assaults. This intensive evidence-based treatment approach, called BRAVEMIND, was originally created by the University of Southern California Institute for Creative Technologies (USC-ICT) in partnership with the U.S. government, for use with soldiers returning from Iraq and Afghanistan. In addition to the visual stimuli

(1) <https://thumbay.com/business-sectors/healthcare>

(2) <https://aimedis.io/metaverseRizzo, A. & Shilling, R., Clinical Virtual Reality tools to advance the prevention, assessment, and treatment. Eur J Psychotraumatol. Published online 2017 Jan 16 https://pubmed.ncbi.nlm.nih.gov/29372007/>

(3) Jacob, N. Neuner, F., Maedl, A., Schaal, S., & Elbert, (2014) Dissemination of psychotherapy for trauma spectrum disorders in postconflict settings: A randomized controlled trial in Rwanda. Psychotherapy and psychosomatics, 83 (6), 354-363.

(4) Iran J Public Health. 2021 Oct;50(10):2046-2054. doi: 10.18502/ijph.v50i10.7505. Effects of Image-Sandplay Therapy on the Mental Health and Subjective Well-Being of Children with Autism; [Juan Guo](#), [Dongmei Li](#), Affiliations expand PMID: 35223572 PMID: [PMC8819219](#) DOI: [10.18502/ijph.v50i10.7505](#)

(5) Frontiers in Psychology. 2017 May 4;8:617. doi: 10.3389/fpsyg.2017.00617. eCollection 2017. Change during Psychotherapy through Sand Play Tray in Children That Have Been Sexually Abused, [Maria D L Angeles Tornero](#), [Claudia Capella](#)

presented in the VR head mounted display, BRAVEMIND uses directional 3D audio, vibrations and even smells which are delivered into an immersive simulation. Rather than relying exclusively on imagining a particular scenario, a patient experiences it again in a virtual world under safe and controlled conditions. Stimulus presentation is controlled by the doctor via a separate interface, with the physician in full audio contact with the patient.

- Wildly successful, the USC-ICT BRAVEMIND program has been expanded for use with civilians. Currently, this system is in use in over 60 clinical sites across the United States (6) and additional use at sites in Canada and Norway. Clinical studies have also been conducted in Brazil to test the efficacy of VRET as an adjunct treatment for patients suffering from panic attacks (7). Clinical VR applications promise to become indispensable tools in the toolbox of psychologists and physicians and will only grow in relevance and popularity in the future.

- What will it take for medical metaverse to be universally adopted? A massive infusion of money to further advance technology is important. Medical device makers are partnering with VR developers to advance the medical metaverse. For example, Spineology, a spinal surgery device maker, has partnered with Ghost Productions, a VR surgical simulation developer, to integrate VR-based training for its sales teams (8). In terms of AR, companies like Aris MD and EchoPixel are looking to gain a foothold in this sector. Aris MD offers 3D visualisations of patient anatomy, allowing the surgeon to perform the procedure in virtual space. Meanwhile, Echopixel creates a ‘digital twin’ of a patient using standard medical images, allowing doctors to experience that image as a ‘4D interactive hologram’.

- On top of the massive financial investment required, some applications are likely to raise privacy concerns. Virtual reality and telemedicine principles are guiding the regulatory framework, but in the United States, additional laws are needed to ensure patient confidentiality and data protection.

- It is expected that the medical metaverse will be a closed world, (meaning that not everyone can access it) and privacy could be improved through greater use of the blockchain. Still, absent the United States finally adopting a comprehensive body of federal privacy and cyber law, widespread use of the medical metaverse will require the use of new technologies to assist it and to ensure patient privacy and confidentiality.

(6) <https://ict.usc.edu/research/projects/bravemind-virtual-reality-exposure-therapy/>

(7) Faria, C., Santos, V., Muniz, M., Do Cabo, M., Nardi, A., & Da Rocha Freire, R. (2021). Virtual reality exposure therapy in panic disorder: A pilot study. *BJPsych Open*, 7(S1), S251-S251. doi:10.1192/bjo.2021.672

(8) Are metaverse applications becoming a reality in medical training? 24 Aug 2022 <https://www.metaverselearning.space/are-metaverse-applications-becoming-a-reality-in-medical-training/>

JANICE F. MULLIGAN

usa@lexing.network



Produits virtuels et jetons non fongibles : dépôt de marques

- L'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) **(1)** a publié, le 23 juin 2022, une communication intitulée « Produits virtuels, jetons non fongibles et métavers » **(2)**.
- Il y présente son approche sur la manière d'appréhender les produits virtuels et les NFT (Non Fungible Token) au regard de la classification de Nice, qui est le document de référence de classification des produits et des services pour les déposants de marques.
- Lors d'une réunion d'information du 24 juin 2022, l'Institut national de la propriété industrielle (INPI) **(3)** s'est également prononcé à ce sujet.

Quelles classes et quelles désignations ?

- Le succès des produits virtuels et des NFT a conduit à l'émergence fulgurante et croissante de dépôts de marques se rapportant à de tels produits.
- Or, la classification de Nice en vigueur **(4)** ne contient pas de libellés officiels en relation avec les produits virtuels et les NFT.
- Jusqu'à présent, ni l'EUIPO, ni l'INPI ne s'étaient exprimés officiellement sur les désignations adéquates conseillés et les classes auxquels rattacher les produits virtuels et les NFT.
- Par conséquent, un flou persistait pour les déposants de marques qui risquaient de se heurter à des objections de l'EUIPO et de l'INPI.
- Les dernières communications de l'EUIPO et de l'INPI sont donc les bienvenues.

La classification des produits virtuels et NFT selon l'EUIPO

- L'EUIPO précise d'abord que les produits virtuels et les jetons non fongibles (NFT) relèvent de la classe 9, dans la mesure où :
 - Les produits virtuels sont analysés comme des « contenus ou images numériques » ;
 - Les NFT sont appréhendés comme des « certificats numériques uniques enregistrés dans une chaîne de blocs qui authentifient des éléments numériques mais qui sont distincts de ces derniers ».
- En revanche, selon l'EUIPO, les désignations « produits virtuels » et « jetons non fongibles » manquent de clarté et de précision et doivent donc être davantage précisées selon les principes suivants.
- S'agissant des produits virtuels, le contenu auquel ils se rapportent doit être explicite, comme dans l'exemple suivant : « produits virtuels téléchargeables, à savoir vêtements virtuels ».

(1) <https://euipo.europa.eu/ohim-portal/fr/web/guest/home>

(2) https://euipo.europa.eu/ohim-portal/fr/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/content/pt-virtual-goods-non-fungible-tokens-and-the-metaverse

(3) <https://www.inpi.fr/>

(4) https://www.wipo.int/classifications/nice/nclpub/en/fr/pdf-download.pdf?lang=fr&tab=class_headings&dateInForce=20210101

- Pour les NFT, l’EUIPO requiert que le type d’élément numérique authentifié par le NFT soit précisé, la seule expression « jetons non fongibles » étant insuffisamment claire et précise.
- Enfin, l’EUIPO souligne que les services se rapportant aux produits virtuels et aux NFT « seront classés conformément aux principes établis de classification de services » d’ores et déjà établis.

La classification des produits virtuels et NFT selon l’INPI

- A l’instar de l’EUIPO, l’INPI classe les produits virtuels et les NFT en classe 9, et estime que les seules désignations « produits virtuels » et « jetons non fongibles (NFT) » manquent de clarté et de précision.
- Pour les produits virtuels, au regard des exemples fournis par l’INPI, le rattachement à une désignation officielle existante s’impose :
 - par exemple, la désignation « objets de collection téléchargeables ou non téléchargeables » est trop floue en raison de la diversité des « objets de collection » ;
 - à l’inverse, la désignation « actifs numériques virtuels téléchargeables » est suffisamment précise, car les actifs numériques sont par ailleurs définis à l’article L.54-10-1 du Code monétaire et financier **(5)** ;
 - de même, le libellé « produits virtuels téléchargeables, à savoir, programmes informatiques en relation avec des parfums, des sacs, des chaussures, des jeux » est suffisamment clair.
- S’agissant des NFT, l’INPI rappelle un principe énoncé par la décision n°2019-157 du Directeur général de l’INPI **(6)** selon lequel un libellé de produits et services ne peut pas comprendre de termes :
 - étrangers,
 - de fantaisie, tels que des marques, ou
 - vagues.
- En conséquence, l’acronyme NFT ne peut pas constituer une désignation acceptable dans un dépôt de marque française.
- De surcroît, la traduction française de NFT, « jetons non fongibles », n’est pas plus acceptable car une telle désignation est équivoque.
- A titre de rappel, un NFT est un « fichier numérique auquel est attaché un certificat d’authenticité numérique c’est-à-dire un jeton cryptographique stocké sur une chaîne de blocs (blockchain) ». Or, si le fichier numérique contenant des vidéos est interchangeable (fongible), tel n’est pas le cas du NFT associé.
- En conséquence, et en accord avec le comité d’experts pour la classification de Nice d’avril 2022, la désignation « jetons non fongibles [NFT] » est remplacée par « fichiers numériques téléchargeables authentifiés par des jetons non fongibles [NFT] ». Il est possible d’être encore plus précis, par exemple en retenant un libellé

(5)
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509570/

(6)
https://www.inpi.fr/sites/default/files/decision_2019-157_depot_et_renouvellement_de_marques_0.pdf

tel que « fichiers d'images téléchargeables contenant des œuvres d'art authentifiées par des jetons non fongibles (NFT) ».

▪ Par ailleurs, conformément à la décision n° 2019-157 précitée, il convient de privilégier les termes « chaîne de blocs » en lieu et place du mot anglais « blockchain ».

La classification des services en lien avec les produits virtuels et NFT par l'INPI

▪ L'INPI a apporté des précisions très utiles sur les libellés des services en relation avec les produits virtuels et NFT.

▪ Par exemple, l'INPI considère les libellés suivants suffisamment clairs et précis :

- « services de magasin de vente au détail en ligne proposant des produits virtuels téléchargeables à savoir, programmes informatiques destinés à être utilisés en ligne et dans des environnements virtuels en ligne » ;
- « services de magasin de vente au détail en ligne proposant des produits virtuels téléchargeables à savoir, programmes informatiques contenant des parfums, des sacs, des chaussures » ;
- « services de divertissement, à savoir mise à disposition de jeux informatiques en ligne destinés à être utilisés dans des environnements virtuels » ;
- « recherche et développement de nouveaux fichiers numériques téléchargeables authentifiés par des jetons non fongibles [NFT] ».

▪ En effet, les services correspondent à des désignations usuelles et se rapportent à des produits clairement identifiables.

▪ Dans la logique de ce qui a été énoncé concernant la classification des produits, l'INPI rappelle que le libellé « vente de jetons non fongibles » n'est pas conforme à la classification de Nice. Il convient donc de privilégier le libellé « service de vente au détail de fichiers numériques téléchargeables authentifiés par des jetons non fongibles [NFT] ».

▪ Par ailleurs, il convient de tenir compte de qu'un « jeton numérique » défini par l'article L.552-2 du Code monétaire et financier **(7)** peut être fongible (crypto-actifs) ou non-fongible (NFT), sans être légalement considéré comme de la monnaie ou des devises (cf. art. L. 54-10-1 du Code monétaire et financier **(8)**). Aussi, le rattachement à la classe 36 ne peut être réalisé que pour des services financiers se rapportant expressément à des services de cryptomonnaie.

(7)
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509545

(8)
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509570/

Evolutions à venir

▪ Les approches adoptées récemment par l'EU IPO et l'INPI sont susceptibles d'évolution.

▪ A noter : Les parties prenantes avaient jusqu'au 3 octobre 2022 pour soumettre leurs observations sur un projet de directives de l'EU IPO pour 2023. Affaire à suivre donc pour les déposants de marques mondes virtuels.

ANNE-SOPHIE
CANTREAU

[france
@lexing.network](https://www.francelexing.com)



Virtual goods and non-fungible tokens: trademark registration

- *The European Union Intellectual Property Office (EUIPO) (1) published a communication entitled “Virtual goods, non-fungible tokens and the metaverse” on 23 June 2022 (2).*
- *In this document, the EUIPO presents its approach on how to deal with virtual goods and NFTs (Non Fungible Tokens) in relation to the Nice Classification, which is the reference document for the classification of goods and services for trademark applicants.*
- *At a briefing on 24 June 2022, the French National Institute of Industrial Property (INPI) (3) also weigh in on this discussion.*

What classes and designations?

- *The success of virtual goods and NFTs has led to a rapid and increasing number of trademark applications relating to such goods.*
- *However, the current Nice Classification (4) does not contain any official wording in relation to virtual goods and NFTs.*
- *Until now, neither the EUIPO nor the INPI has officially expressed an opinion on the appropriate designations and classes to which virtual goods and NFTs should be attached.*
- *As a result, a lack of clarity persisted for trademark applicants who risked objections from the EUIPO and INPI.*
- *The latest communications from the EUIPO and the INPI are therefore welcome.*

The EUIPO’s classification of virtual goods and NFTs

- *The EUIPO first clarifies that virtual goods and non-fungible tokens (NFTs) are proper to Class 9, because:*
 - *Virtual goods are treated as “digital content or images”;*
 - *NFTs are treated as “unique digital certificates registered in a blockchain, which authenticate digital items but are distinct from those digital items”.*
- *However, in the EUIPO’s view, the terms “virtual goods” and “non-fungible tokens” lack clarity and precision and therefore need to be further specified.*
- *For virtual goods, the content to which they relate must be made explicit, as in the following example: “downloadable virtual goods, namely, virtual clothing”.*
- *For NFTs, the EUIPO requires that the type of digital item authenticated by the NFT be specified, as the term “non-fungible tokens” on its own is insufficiently clear and precise.*

(1) <https://euipo.europa.eu/ohim-portal/>

(2) https://euipo.europa.eu/ohim-portal/en/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/content/pt-virtual-goods-non-fungible-tokens-and-the-metaverse

(3) <https://www.inpi.fr/>

(4) https://www.wipo.int/classifications/nice/nclpub/en/fr/pdf-download.pdf?lang=fr&tab=class_headings&dateInForce=20210101

▪ The EUIPO stresses that services relating to virtual goods and NFTs “will be classified in line with the [already] established principles of classification for services”.

The INPI’s classification of virtual goods and NFTs

▪ Like the EUIPO, the INPI classifies virtual goods and NFTs in Class 9, and considers that the terms “virtual goods” and “non-fungible tokens (NFTs)” alone lack clarity and precision.

▪ For virtual goods, it follows from the examples provided by the French office that a link to an existing official designation is necessary:

- for example, the terms “downloadable or non-downloadable collectibles” is too vague because of the diversity of “collectibles”;
- conversely, the terms “downloadable virtual digital assets” is sufficiently precise, to the extent that digital assets are defined in Article L.54-10-1 of the French Monetary and Financial Code **(5)**;
- similarly, the wording “downloadable virtual products, namely computer programs related to perfumes, bags, shoes, games” is sufficiently clear.

▪ For NFTs, the INPI recalls a principle set out in Decision No. 2019-157 of the Director General of the INPI **(6)** according to which a description of goods and services may not include terms that are:

- foreign,
- fanciful (such as trademarks), or
- vague.

▪ Consequently, the acronym NFT cannot constitute an acceptable designation in a French trademark application.

▪ The translation into French of NFT, “jetons non fongibles”, is no more acceptable as such a designation is equivocal.

▪ As a reminder, an NFT is a “digital file to which is attached a certificate of digital authenticity, i.e. a cryptographic token stored on a blockchain”. While the digital file containing videos is interchangeable (fungible), the associated NFT is not.

▪ Consequently, and in agreement with the Committee of Experts of the Nice Union of April 2022, the designation “non-fungible tokens [NFT]” is replaced by “downloadable digital files authenticated by non-fungible tokens [NFT]”. It is possible to be even more precise, for example by using a wording such as “downloadable image files containing works of art authenticated by non-fungible tokens (NFT)”.

▪ Furthermore, in accordance with the above-mentioned Decision No. 2019-157, the French terms “chaîne de blocs” should be used instead of the English word “blockchain”.

(5)
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509570/

(6)
https://www.inpi.fr/sites/default/files/decision_2019-157_depot_et_renouvellement_de_marques_0.pdf

The INPI's classification of services related to virtual goods and NFTs

- The INPI has provided very useful clarification on the wording of services in relation to virtual products and NFTs.
- For example, the INPI considers the following wordings sufficiently clear and precise:
 - “online retail shop services offering downloadable virtual goods namely, computer programs for use online and in online virtual environments”;
 - “online retail shop services offering downloadable virtual goods, namely computer programs containing perfumes, bags, shoes”;
 - “Entertainment services, namely provision of online computer games for use in virtual environments”;
 - “research and development of new downloadable digital files authenticated by non-fungible tokens [NFT]”.
- These services correspond to usual designations and relate to clearly identifiable goods.
- In line with what has been stated concerning the classification of goods, INPI points out that the wording “sale of non-fungible tokens” does not comply with the Nice Classification. The wording “retail service of downloadable digital files authenticated by non-fungible tokens [NFT]” should therefore be preferred.
- It should further be taken into account that a “digital token”, as defined by Article L.552-2 of the Monetary and Financial Code **(7)**, may be fungible (crypto-assets) or non-fungible (NFTs), without being legally considered as money or currency (Article L. 54-10-1 of the Monetary and Financial Code **(8)**). Therefore, the connection to class 36 can only be made for financial services that are expressly related to cryptocurrency services.

Next steps

- The positions recently adopted by the EUIPO and the INPI are subject to change.
- Stakeholders had until 3 October 2022 to submit comments on the approach set out in the EUIPO's 2023 draft Guidelines. Applicants for trade marks in the virtual worlds should stay tuned for updates.

(7)

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509545

(8)

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509570/

ANNE-SOPHIE
CANTREAU

[france](#)
[@lexing.network](#)



Métavers et protection des consommateurs

Le présent article offre une analyse succincte du régime juridique de la protection des consommateurs dans le métavers : il identifie les éléments de base du cadre juridique actuel, examine son application possible aux différents composants du métavers, et recense ou anticipe les problèmes associés.

- Le droit de la consommation, qui régit les relations entre les consommateurs et les professionnels est vaste et couvre une multitude de domaines, tels que la responsabilité du fait des produits, les pratiques commerciales déloyales, la publicité trompeuse et comparative, ainsi que les pratiques commerciales agressives qui vont de la contrainte au harcèlement en passant par l'influence injustifiée **(1)**. Il se situe également au carrefour de plusieurs autres branches du droit, aussi diverses que la protection des données et de la vie privée, la responsabilité délictuelle, le droit pénal ou le droit administratif.
- Univers virtuel, le métavers héberge une kyrielle d'applications et de services censés améliorer la réalité physique, et constitue un nouvel environnement où se rencontrent consommateurs et professionnels pour s'y échanger toutes sortes de produits et services.
- L'arsenal législatif complet et complexe de la protection des consommateurs d'ores et déjà en place dans l'Union européenne va devoir évoluer pour pouvoir s'appliquer aux métavers. Dans certains cas, cette opération pourra se faire sans trop de difficultés. Par exemple, la règle selon laquelle le producteur est responsable du dommage causé par un défaut de son produit pourrait prendre en compte les dommages immatériels **(2)**.
- Dans d'autres cas, la tâche sera plus ardue. Ainsi, la porosité entre les différentes identités existant dans le métavers pourrait rendre délicate la distinction entre contenu utilisateur et contenu commercial, ce qui n'est pas sans conséquence. Prenons un exemple : un avatar faisant l'éloge d'une marque dans le métavers tombe-t-il sous le coup de la réglementation en matière de publicité trompeuse, protectrice des consommateurs, ou peut-il y échapper au titre de l'exercice de la liberté d'expression **(3)** ? La législation actuelle est déjà apparue obsolète dans certains cas, notamment pour encadrer les influenceurs ou encore les humains virtuels. Ces derniers sont des agents artificiels composés à la fois d'un corps virtuel à apparence humaine et d'une composante cognitive capable de prendre des décisions et de contrôler les comportements pour réaliser dans des activités semblables à celles des humains **(4)**.
- En outre, le métavers remet en cause la pertinence de certains concepts du droit à la consommation, tels que « contrats à distance », utilisés dans le cadre de ventes sur internet **(5)**. En effet, même si, dans le métavers, les consommateurs pourront acquérir des produits ou des services d'une manière assez similaire à la

(1) Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur (directive sur les pratiques commerciales déloyales)

(2) Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux (telle que modifiée)

(3) Directive 2006/114/CE du Parlement européen et du Conseil du 12 décembre 2006 en matière de publicité trompeuse et de publicité comparative

(4) Traum. D. (2009). Models of culture for virtual human conversation

(5) Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs

vie hors ligne, cet achat relèvera légalement de la définition des contrats « à distance et hors établissement ». Comment certaines clauses contractuelles (relatives aux obligations d'information, aux obligations formelles ou au droit de rétractation) vont-elles alors s'appliquer dans le métavers ?

▪ Enfin, une autre question devient de plus en plus prégnante : celle des « *dark patterns* » **(6)**, c'est-à-dire les interfaces truquées utilisées par les fournisseurs de services en ligne pour inciter (de manière plus ou moins forte) les utilisateurs à prendre certaines décisions. De récentes initiatives législatives de l'Union européenne visent à limiter ces pratiques. En particulier, la législation sur les services numériques (également connue sous sa désignation anglaise « Digital Services Act ») **(7)** condamne plusieurs pratiques assimilables aux *dark patterns*, comme le fait de demander fréquemment ou avec insistance aux utilisateurs de prendre une décision ou de modifier un paramètre du service après que l'utilisateur a déjà fait un choix. Gageons que si ces dispositions ne visent pas pour l'instant expressément les acteurs du métavers, ces derniers seront bien amenés, à terme, à s'y conformer.

(6) Lignes directrices du comité européen de la protection des données (CEPD-EDPB) : « Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them »

(7) Proposition de règlement du Parlement européen et du Conseil du relatif à un marché intérieur des services numériques (Législation sur les services numériques)

GEORGE A.
BALLAS
&
NIKOLAOS
PAPADOPOULOS

[greece@
lexing.network](mailto:greece@lexing.network)



Metaverse and Consumer protection

This is a high-level analysis of the consumer protection legal framework in the Metaverse. We aim to identify the basic elements of the current legal framework of consumer protection legislation, its application on elements of the metaverse, and potential legal issues and controversies.

- *Consumer protection legislation governs the relationships between individual consumers and businesses, covering areas such as product liability, unfair commercial practices, misleading and comparative advertising, as well as aggressive commercial practices, spanning from coercion to harassment and undue influence (1). At the same time, consumer protection legislation intersects with other areas of law, such as data protection, privacy, tort, and even criminal or administrative legislation.*
- *The Metaverse is a virtual universe enhancing countless aspects of physical reality, hosting endless applications and limitless possibilities, permeated by individuals falling within the definition of consumer, as well as business practices offering their products and services in this novel digital environment.*
- *In this respect, the complex and comprehensive legal framework of consumer protection in the European Union will need to adapt in the realm of Metaverse. In some cases, the application of relevant provisions appears rather straightforward; for example, producers being liable for any damage incurred by their defective products to consumers, also encompassing liability for non-material damages (2).*
- *To some extent, the blurring lines between different identities in the Metaverse would raise obstacles to distinguishing between user content and business content, essentially between the freedom of expression and the regulatory restrictions of consumer protection legislation. For example, an avatar praising a brand in the Metaverse could fall within the description of misleading advertising, or under the exercise of the freedom of expression (3). The standards set out by legislation have been deemed as already obsolete in certain cases, arguably with the phenomenon of influencers and most prominently with virtual humans, i.e. artificial agents that include both a visual body with a human-like appearance and a range of observable behaviours and a cognitive component that can make decisions and control the behaviours to engage in human-like activities (4).*
- *Meanwhile, the Metaverse obfuscates terms such as “distance contracts”, which are used for sales via the Internet (5). Arguably, in the Metaverse, consumers will be able to obtain products or acquire services in a way closely resembling offline life but legally within the definition of “distance and off-premises” contracts. It remains to be seen how clauses such as those covering the information*

(1) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive')

(2) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (as amended)

(3) Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising

(4) Traum, D. (2009). Models of culture for virtual human conversation

(5) Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights

requirements, the formal requirements or the right of withdrawal will apply in the Metaverse.

▪ Finally, another issue gaining traction is the dark patterns **(6)**, used by online service providers to nudge or pressure users towards making particular decisions. Recent legislation initiatives of the European Union aim to restrict this phenomenon, namely via the provisions of the Digital Services Act **(7)**, which delineates various practices amounting to dark patterns, including repetitively requesting or urging users to make a decision or to change a setting after the user has already made a choice. Such provisions for the time being do not specifically target providers in the Metaverse, but will eventually need to take them into account.

(6) European Data Protection Board (EDPB) Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them

(7) Proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act)

GEORGE A.
BALLAS
&
NIKOLAOS
PAPADOPOULOS

[greece@
lexing.network](mailto:greece@lexing.network)



Métavers et vie privée

- A l'instar du mot « robot », inventé par l'écrivain tchèque Karel Capek en 1920 dans une pièce de théâtre intitulée R.U.R, le terme « métavers » est également issu d'une œuvre littéraire, le roman de science-fiction « Snow crash » (traduit en français sous le titre « Le Samouraï virtuel »), écrit en 1992 par l'américain Neil Stephenson. Mais alors que les robots sont parmi nous depuis des décennies, le métavers entre tout juste en scène. Pourtant, il ne fait aucun doute que le métavers connaisse une croissance spectaculaire, en raison de la numérisation continue de notre société, des progrès technologiques constants et de la généralisation des plateformes numériques. Les plateformes, justement, sont des acteurs de premier plan dans le métavers, car ce sont à travers elles que les utilisateurs communiquent et interagissent entre eux. Ces plateformes sont utilisées aussi bien par des entités privées que publiques, que pour des usages professionnels et personnels. Il suffit d'évoquer les assistants numériques qui, avec notre consentement tacite, ont été introduits dans nos foyers où ils recueillent une quantité importante de données sur la vie privée de leurs utilisateurs.
- Le métavers est un espace virtuel en 3D, capable d'interagir avec le monde physique et pouvant être partagé par plusieurs utilisateurs (grâce aux plateformes). Avec des avatars, les utilisateurs entrent dans le métavers où ils peuvent se mettre en relation avec d'autres utilisateurs ou utiliser des fonctionnalités et applications (commerciales ou ludiques) disponibles dans cet espace virtuel.
- Le métavers s'accompagne d'un nouveau vocabulaire auquel il va falloir nous habituer, tels que réalité virtuelle (RV), réalité augmentée (RA) et jumeaux numériques. La RV crée l'espace virtuel dans lequel les utilisateurs sont totalement immergés, tandis que la RA permet l'interaction avec la réalité physique. Quant aux jumeaux numériques, ce sont des copies numériques d'objets physiques, qui sont introduites dans la RV pour y être partagées ou testées : par exemple, les ingénieurs qui développent un produit peuvent, grâce au jumeau numérique de ce produit, utilement tester ses fonctionnalités et ses capacités, en découvrir les faiblesses potentielles et tous autres problèmes, avant que le produit n'entre en phase de fabrication et ne soit mis sur le marché.
- Tous les secteurs d'activité sont concernés par le métavers : les affaires, le commerce, l'éducation et l'apprentissage, sans oublier l'interaction sociale et les jeux. Tous ces marchés promettent des opportunités commerciales énormes. Si le potentiel est clair, la quantité et la nature des nouvelles technologies révolutionnaires qui seront développées par et pour le métavers reste encore inconnues.

- Même si le métavers n'est qu'à un stade embryonnaire, nombreux sont ceux qui s'inquiètent déjà des risques qu'il implique pour la vie privée. Alors que nous ne connaissons pas encore toutes les technologies qui graviteront autour du métavers, et donc les risques inhérents à celles-ci, on peut néanmoins d'ores et déjà en esquisser certains dangers potentiels.

- Dans le monde numérique d'aujourd'hui, internet, les réseaux sociaux et les différentes technologies existantes alimentent les bases de données des spécialistes du marketing par une quantité astronomique de données personnelles, allant jusqu'à la façon dont nous bougeons notre souris. Par exemple, lorsque vous faites des recherches pour acheter un billet d'avion en ligne, le prix affiché peut être sensiblement différent en fonction du lieu et de l'heure d'achat (un achat après les heures de travail indique que vous possédez votre propre ordinateur) et de la marque de votre ordinateur (si vous avez un Mac, vous paierez un prix plus élevé que si vous aviez un PC). Autre exemple : votre historique de navigation est une source majeure de données. Le simple classement des informations vous concernant dénichées dans votre historique de navigation dans quatre grandes catégories utilisées par la plupart des réseaux sociaux (adorer, aimer, détester, croire) suffit aux spécialistes du marketing pour dresser votre portrait-robot complet : de votre équipe de football préférée à vos convictions politiques ou religieuses, en passant par vos préférences alimentaires et vos choix en matière de divertissement. Le métavers, qui est particulièrement intrusif, va élargir davantage le spectre des données personnelles déjà disponibles.

- En effet, pour donner à l'utilisateur la sensation d'une immersion totale dans le métavers ainsi que la possibilité d'interagir avec d'autres utilisateurs, le dispositif de RV et la plateforme lui envoient des stimuli visuels. La plateforme, et éventuellement le fabricant du dispositif, ont donc accès à des données sur la localisation et la marque de l'ordinateur de l'utilisateur. Or, ces données peuvent à elles seules révéler le niveau de richesse de l'utilisateur. Des dispositifs plus sophistiqués collectent également des informations sur l'état physique de l'utilisateur, telles que la taille, la longueur et l'envergure de ses bras. En outre, l'observation de la réaction aux stimuli envoyés (temps de réaction, manière de se déplacer) pourraient facilement faire apparaître en filigrane le degré de forme physique et l'âge de l'utilisateur. D'autres informations, encore, décrivent la pièce, ou plus généralement l'environnement, dans lequel il évolue. Loin d'être exhaustive, la liste des informations potentiellement accessibles par le biais du métavers dressée ici peut s'allonger à l'infini. Dès lors, une conclusion se dégage : toutes ces informations sont clairement beaucoup plus personnelles et intrusives pour la vie privée d'un utilisateur que n'importe quelles informations personnelles actuellement obtenues par le biais de l'Internet 2.0.

- Dans ce contexte, la question qui s'impose est donc : sommes-nous prêts ? Plus concrètement, cette question se décline, d'un point de vue de l'utilisateur, en « comment protéger ma vie privée ? » et, du point de vue du responsable du traitement de ces données « comment assurer ma conformité au RGPD ? ».

- Une chose est sûre : avec le métavers, la protection de la vie privée ne peut pas être abordée de la même manière que celle utilisée jusqu'à présent. La complexité de cette nouvelle technologie (pour le peu que nous connaissions aujourd'hui, et donc sans compter sur ses évolutions futures) et l'ampleur de ses risques potentiels pour la vie privée exigent un changement de paradigme. En tout état de cause, les entreprises qui proposent des produits ou des services dans le métavers doivent être particulièrement vigilantes et veiller à dûment informer les utilisateurs des informations qu'elles collectent, des finalités auxquelles elles sont destinées, etc.
- Les responsables du traitement (et les autorités) vont devoir adopter une autre approche, qui ne se mesure pas uniquement à l'aune de la conformité au RGPD. Ils ne pourront pas se contenter de contrôler qui utilise les données personnelles dont ils ont besoin pour mener leurs activités, et comment ils les utilisent : ils devront contrôler la gouvernance des données, ce qui implique de passer à une approche globale incluant toutes les facettes des processus multicouches du métavers : sources de données, flux d'informations, spécifications des dispositifs, contrôle du réseau, accès aux données, etc.
- Le monde sera bien différent lorsque le métavers aura atteint son plein potentiel, et les questions juridiques qui en découleront risquent de mobiliser les acteurs du monde juridique à long terme. La route vers le métavers s'annonce donc mouvementée, mais exaltante, pour les avocats spécialisés dans les technologies avancées.

RAFFAELE ZALLONE

[italy@
lexing.network](mailto:italy@lexing.network)



Privacy in the Metaverse

- *The word “robot” was invented by Karel Capek, a Czech writer who used it in 1920 in a theatre play called R.U.R. In the same fashion the expression “metaverse” was used for the first time in a science-fiction novel called “Snow crash”, written in 1992 by Neil Stephenson. But while robots have been used for decades now, the Metaverse is still in its early stage. Yet, there is no doubt that metaverse is bound towards a very, very significant growth, due to the continuous digitalization of our society, to the increasing advances in technology and with the spread of digital platforms. Platforms will be very important in the metaverse since they will allow users to communicate and interact with each other. These platforms are wide-based, i.e. used for professional applications by businesses or public entities, as well as private-based, such as the digital assistants that, with our silent consent, have been introduced in many households and have helped to gather significant amount of data related to the private lives of their users.*
- *Metaverse is a 3D virtual space, capable of interacting with the physical world; a space that can be shared between many users (thanks to the platforms, as I said above). Users shall enter the metaverse with avatars and create liaisons with other users or they shall be able to use the functionalities and applications (business or gaming) available in the virtual space.*
- *With the growth of Metaverse we shall get accustomed with words and concepts like Virtual Reality (VR), Augmented Reality (AR) and Digital Twins. The VR will create the virtual space where users will be fully immersed in, while AR will allow the interaction with physical reality; finally, Digital Twins are digital copies of physical objects, that will be brought into the VR and either shared or tested: for example, engineers developing a product through the digital twin of the new product will be able to test its functionalities and capabilities, discovering potential weaknesses and other issues, before launching the product gets in manufacturing stage and enters the marketplace.*
- *Metaverse will be used for many purposes: for business or for commerce, for education and learning, not to mention for social interaction and gaming; all these markets promise potentially enormous business opportunities. But while the potential is clear, what we still do not know now is the amount and the nature of the new and revolutionary technologies that shall be developed and that we can only imagine today.*
- *In this scenario, even if metaverse is at an early stage of development, many authors have already pointed out the inherent risks and challenges with respect to the privacy of the users. Let’s then have a look at what these dangers seem to be:*

I use the word “seem” since, as I said, at this time we are aware only of some of technologies that we will face in the future.

▪ *In today’s digital world, Internet, social interaction and existing technologies have given marketers a wealth of information: from the way we use the mouse to many other personal information. For example, if you buy an airplane ticket the price may be significantly different based on a number of factors. Price may vary depending on time and venue of purchase, because if you buy it after work hours, it means you have access to your own computer. The brand of your computer has a reflection of price: if you have a Mac you’re bound to pay a different, higher price as compared to a buyer who owns a PC. Surfing history gives indication of what product you like; some social networks used just four words to create a user’s profile: love, like, hate, believe. These simple words have told marketers everything from our preferred soccer team to our political or religious beliefs, from our preferred food to our entertainment choices. Metaverse will allow access to a much greater set of information; indeed, it shall also provide access to a more pervasive set of information.*

▪ *VR devices allow users to have the feeling of full immersion in the virtual space; the platform and the device provide visual stimuli to the user, who then interacts with other users. The platform and possibly the manufacturer of the device have access to data as positioning, the brand of the user host computer, who in turn may give hints on the wealth of the user. More sophisticated devices can detect physical information such as height, arm length and wingspan. Behavioral observation of the reaction to the stimuli gives access to another set of private information: observing how a user reacts to pre-determined stimuli can reveal significant information on the user’s behavior and personality. Based on reaction time and depending on how the user moves, the device could give additional personal, physical information: the degree of his/her fitness and the age of the user could be easily determined; other information could be related to the environment where the user operates. The list of potential information available through the metaverse could go on and on, and points to one conclusion: all this information is clearly much more personal and invasive of a user’s privacy than any set of personal information that can presently be obtained through Internet 2.0.*

▪ *The question is then: do we have the means to prevent this invasion of users’ lives? Looking at the same issue from another angle, what should a controller do to be GDPR compliant?*

▪ *One point is clear: in this environment, privacy issues cannot be addressed with the same approach we have used so far for today, existing privacy issues. The complexity of this new technology (and, as I said, considering that we are only know the little that exist today) and the amount of its potential privacy risks require a totally different approach. Therefore all the companies offering products or services in the metaverse have an obligation to duly inform the users of what information they collect, how they use them, for what purposes, etc, because users must be clearly aware of the privacy implications and make conscious decisions.*

- *The approach of controllers (as well as authorities) must concentrate on a different concept as compared to the need to comply with GDPR. They cannot simply control who uses personal information they need to conduct their business and how: they must address and control overall data governance, that implies switching to a global approach that includes all facets of the multi-layered processes of Metaverse: data sources, information flows, devices specifications, network control, data access, etc.*
- *The world will be quite different when metaverse will have reached its true potential, and the legal challenges involved will keep us busy for quite a while. It's a bumpy ride, but at the same time an exciting new adventure for the leading-edge technology lawyers.*

RAFFAELE ZALLONE

[italy@
lexing.network](mailto:italy@lexing.network)



Le futur, c'est maintenant !

Du pouvoir disruptif de l'IA et de ses ramifications juridiques dans le métavers

- L'IA est probablement l'une des technologies les plus évolutives de l'histoire. Elle porte l'incroyable potentiel de remodeler entièrement les fondements de l'ensemble des secteurs d'activité, de générer une croissance économique spectaculaire et de modifier à jamais notre façon de vivre et d'interagir les uns avec les autres.
- Le métavers, qui repose pour une grande part sur les technologies de l'IA, est annoncé comme allant révolutionner à son tour les interactions humaines sur les nouvelles plateformes de médias sociaux et la connexion aux équipements de divertissement, de jeu et de travail dans le cyberspace. Malgré les défis auxquels les grandes entreprises technologiques sont confrontées pour le moment dans ce nouveau monde, le métavers est en train de gagner son statut d'« Internet nouvelle génération » en constituant déjà un lieu multidimensionnel de rencontre, de travail et de commerce pour un nombre croissant d'utilisateurs.
- Dans ce contexte, comment se met en place la future réglementation en matière d'IA et de métavers au Royaume-Uni ?

IA, métavers et protection des données au Royaume-Uni

- Le RGPD et les textes équivalents applicables post-Brexit au Royaume-Uni (UK GDPR, loi sur la protection des données de 2018) encadrent expressément le traitement automatisé à grande échelle de données personnelles. A ce titre, le déploiement des technologies de suivi reposant sur l'IA et utilisées dans le métavers font l'objet d'une surveillance étroite par les régulateurs. Les articles 13 et 14 du RGPD consacrent le droit, pour les personnes concernées, d'être informées (i) de l'existence d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques les concernant ou les affectant de manière significative, (ii) de la logique sous-jacente et (iii) de l'importance et des conséquences prévues pour ces personnes.
- L'article 15 du RGPD, quant à lui, leur confère un droit d'accès (i) aux informations sur l'existence d'une prise de décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques les concernant ou les affectant de manière significative, (ii) aux informations utiles concernant la logique sous-jacente et (iii) à l'importance et aux conséquences prévues de ce traitement pour les personnes concernées. Enfin, l'article 35 du RGPD introduit l'obligation d'effectuer une analyse d'impact relative à la protection des données (AIPD) lorsque le traitement des données à caractère personnel, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les personnes physiques (profilage systématique et approfondi, ou toute autre évaluation qui est fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire). Il

s'ensuit que la réalisation d'une AIPD va probablement être imposée en cas de traitement des données personnelles par des systèmes d'IA dans le métavers.

Le futur cadre réglementaire de l'IA au Royaume-Uni

- Alors que l'IA est déjà parmi nous, le métavers a tout pour faire également partie de notre quotidien, et le législateur britannique se doit d'agir pour garantir à chaque secteur économique la possibilité d'en exploiter toutes les potentialités. Les pouvoirs publics doivent suivre le rythme de la technologie et s'adapter à l'évolution rapide de l'IA et du métavers pour maximiser la croissance, favoriser la concurrence et promouvoir l'innovation, tout en protégeant la sûreté, la sécurité, et les droits des personnes.
- Le Royaume-Uni, qui a pour ambition de se positionner comme un acteur mondial dans le domaine de l'IA, s'est donné pour objectif stratégique de devenir le centre de la recherche et de l'innovation en la matière, de constituer un réservoir de talents mondiaux et de créer un écosystème réglementaire et commercial dynamique. La Stratégie Industrielle, qui exposait dès 2017 le plan du gouvernement en ce sens, a ainsi rendu possible la réalisation de multiples projets dans le domaine de l'IA.
- En avril 2018, le gouvernement britannique et les acteurs de l'IA ont conclu un accord sectoriel sur l'IA de près d'un milliard de livres sterling dans le but de renforcer la position mondiale du Royaume-Uni en tant que leader dans le développement des technologies de l'IA, qui sont des technologies de premier plan dans le métavers. Enfin, le dernier texte en date relatif à la stratégie nationale en matière d'IA, amorce un changement de direction en entérinant la capacité du métavers à constituer, via l'IA, un espace d'innovation pour les acteurs privés et publics.

Les enjeux liés à la propriété intellectuelle

- L'avènement de l'IA dans les industries artistiques et créatives, et plus particulièrement dans le métavers, est une gageure pour le droit de la propriété intellectuelle. Les œuvres générées par l'IA (jeu vidéo, peinture, musique, photographie, vidéo) peuvent, en effet, modifier les définitions de créateur, d'auteur et d'inventeur que l'on croyait pourtant fermement établies.
- Il n'y a pour le moment aucune certitude juridique quant à la manière de traiter et de protéger correctement les œuvres générées par l'IA. Des concepts tels que la juste récompense et les droits moraux pourraient potentiellement être mobilisés pour « rémunérer » les inventions ou les créations générées par une IA. Cette démarche se heurte toutefois au principe actuel selon lequel seules les personnes physiques sont capables de créer intentionnellement une œuvre d'art et, par conséquent, elles seules peuvent se voir octroyer des droits de propriété intellectuelle sur ces créations. L'application stricte des lois existantes sur le droit d'auteur au contenu créé par l'IA aboutit à une protection insuffisante dans la mesure où elle « exclut » le robot : le programmeur informatique humain, et lui seul, se voit conférer des droits mais uniquement sur le code qui a permis à la machine de créer artificiellement l'œuvre protégée par le droit d'auteur, et pas sur l'œuvre elle-même.

▪ Au vu de la rapidité et de l'importance des changements provoqués par l'utilisation des technologies d'IA dans les industries créatives, plusieurs concepts traditionnels du droit de la propriété intellectuelle (créations artistiques, inventions, marques) risquent d'être fréquemment bousculés. Le cadre réglementaire doit s'adapter rapidement à ce nouveau paradigme. Il sera peut-être également nécessaire de repenser entièrement la notion de « création ». A cet effet, on pourrait utilement dresser l'inventaire des droits et obligations (le cas échéant) inhérents à ces nouvelles expressions créatives, telles qu'elles sont comprises par les humains, analyser les modalités selon lesquelles elles pourraient être qualifiées de nouvel objet protégeable (à supposer qu'une œuvre créée par l'IA puisse être classée comme telle), et déterminer si l'intention humaine doit continuer à être une condition préalable à une création artistique. A défaut, les œuvres d'IA créées dans le métavers pourraient entrer directement dans le domaine public, fragilisant ainsi davantage la relation auteur-consommateur.

DANIEL PREISKEL
&
XAVIER PRIDA

[uk@
lexing.network](mailto:uk@lexing.network)



The Future Is Now:

The Disruptive Power of AI and Its Legal Ramifications in The Metaverse

- *AI is perhaps one of the fastest evolving technologies ever devised, with enormous capabilities to entirely reshape the very foundations of a range of businesses, enable significant financial development and forever alter our way of living and interacting with one another.*
- *There are high expectations that the metaverse, which relies greatly on AI technologies, will in turn revolutionise how users interact with one another within new social media platforms and how they connect to entertainment, gaming and work devices in the cyberspace. Despite the challenges that major tech companies are facing at the time of writing, the metaverse is indeed harnessing its status as the next generation of the internet, already enabling the growing number of users to socialise and work in a virtual world all the while making real life financial transactions within the multidimensional system.*
- *This short form article touches on a couple of UK legal aspects and issues shaping future regulation of AI and the Metaverse.*

AI and Metaverse UK Data Protection Aspects

- *Both the GDPR and the UK's retained version of the GDPR, including the Data Protection Act 2018 have a significant focus on large scale automated processing of personal data and as such the deployment of AI tracking technologies in the metaverse will be ever scrutinised by the regulators. Articles 13 and 14 of the GDPR deal with the right to be informed of: (i) the existence of solely automated decision-making producing legal or similarly significant effects; (ii) meaningful information about the logic involved; and (iii) the significance and envisaged consequences for the individual.*
- *Article 15 of the GDPR on the other hand regulates the right of access to: (i) information on the existence of solely automated decision-making producing legal or similarly significant effects; (ii) meaningful information about the logic involved; and (iii) the significance and envisaged consequences for the individual. Article 35 of the GDPR further addresses the so-called Data protection impact assessments ("DPIAs") whereby organisations must carry out DPIAs if their processing of personal data, particularly when using new technologies, is likely to result in a high risk to individuals. (i.e., any systematic and extensive profiling or other automated evaluation of personal data which are used for decisions that produce legal or similarly significant effects on people). DPIAs are therefore likely to be an obligation for using AI systems to process personal data in the metaverse.*

The Impending AI Regulatory Framework in the UK

- *As AI is already becoming part of everyday life and the potential of the metaverse in a wide variety of industries, legislative action is required in order to guarantee that every sector benefits from their use. Policies and regulatory frameworks accordingly need to keep pace with the fast-changing demands of AI and the expansion of the metaverse, with the purpose of not only maximising growth and*

competition, promoting innovation, but also protecting the safety, security, choices and rights of users.

- *The UK in particular considers itself to be a global force in AI and is strategically situated to pave the way over the next decade as an authentic research and innovation capital, a centre of global talent and a flourishing regulatory and business ecosystem. Various of the UK's achievements in AI were enabled by the 2017 Industrial Strategy, which laid out the government's plan to turn the UK into a global hub for the AI revolution.*

- *In April 2018, the government and the UK's AI ecosystem agreed a near £1 billion AI Sector Deal to boost the UK's global position as a leader in developing AI technologies which are so deeply intertwined with the metaverse. The latest National AI Strategy signifies a shift in direction for AI in the UK, acknowledging its capabilities in the metaverse in order to foster an expanding innovative space in both the private and public spheres.*

Intellectual Property

- *The advent of AI in the artistic and creative industries, most notably in the metaverse sector, will continue to pose a series of challenges to the underlying principles of intellectual property law. For instance, AI generated works such as videogames, paintings, music, photography and video can indeed alter the established concepts of the creator, author and inventor.*

- *While there are no legal certainties as to how to deal and properly protect AI generated works, concepts such as just reward, and moral rights could potentially be applied to "compensate" AI-generated inventions or creations. This, however, contravenes the notion that only human beings are genuinely capable of intentionally creating a work of art, and therefore only they can be granted Intellectual Property Rights ("IPR") over their creations. By strictly applying existing copyright laws to AI-created content, the protection falls short inasmuch as it "excludes" the robot with only the human computer programmer being awarded rights in relation to the code that enabled the machine to artificially create the copyrightable work, but technically not over the resulting work itself.*

- *On account of these fast-paced changes brought about by the use of AI technologies in the creative industries, traditional IP concepts such as artistic creations, inventions, and presumably even trademarks, amongst other works, will be continuously put to the test and the regulatory framework must therefore quickly adapt to the new paradigm. Perhaps the mere notion of what makes up a creation at its most basic may also have to be redefined. This could comprise analysing the scope of rights and obligations (if any) that are inherent to these creative expressions, as understood by humans, and how they may qualify as a new protectable subject matter (if an AI created work can even be classified as such), and whether or not the human intent should continue to be a prerequisite of an artistic creation. In any event, the lack of definition may pave way for AI works created in the metaverse to directly enter into the public domain and further disrupt the author-consumer relationship.*

DANIEL PREISKEL
& XAVIER PRIDA

[uk@
lexing.network](mailto:uk@lexing.network)

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud <i>South Africa</i>	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne <i>Germany</i>	Mercatorius	Guido Imfeld	+49(0)241 / 946 21-0	germany@lexing.network
Australie <i>Australia</i>	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique <i>Belgium</i>	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Brésil <i>Brazil</i>	Opice Blum, Bruno e Vainzof Advogados	Andrea Filomeno Faria	+55 11 2189 0061	brazil@lexing.network
Canada <i>Canada</i>	Langlois avocats, S.E.N.C.R.L.	Cynthia Chassigneux	+1 (418) 650 7000	canada@lexing.network
Chine <i>China</i>	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Côte d'Ivoire <i>Ivory Coast</i>	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne <i>Spain</i>	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis <i>USA</i>	Mulligan, Banham & Findley	Janice F. Mulligan	+1 619.238.8700	usa@lexing.network
France <i>France</i>	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce <i>Greece</i>	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Hongrie <i>Hungary</i>	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde <i>India</i>	Poovayya & Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Italie <i>Italy</i>	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon <i>Japan</i>	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban <i>Lebanon</i>	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Luxembourg <i>Luxembourg</i>	Emmanuelle Ragot Lawyers & Associates	Emmanuelle Ragot	+ 352 661 84 4250	luxembourg@lexing.network
Maroc <i>Morocco</i>	Elkhatib Lawfirm	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique <i>Mexico</i>	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De González Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège <i>Norway</i>	Advokatfirmaet Føyen AS	Knut Fiane	+47 21 93 10 00	norway@lexing.network
Philippines <i>Philippines</i>	Calleja Peralta Jimenez San Luis Uy & Ulibas (Calleja Law Office)	Anthony B. Peralta	+6336113 +6352307	philippines@lexing.network
République tchèque <i>Czech Republic</i>	Rowan Legal	Michal Nulicek Josef Donat	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni <i>United Kingdom</i>	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Rwanda <i>Rwanda</i>	Siewe William Walter	Siewe William Walter	+(250) 787 642 337	rwanda@lexing.network
Sénégal <i>Senegal</i>	SCP Faye & Diallo	Mamadou Seye	(+221) 33 823 60 60	senegal@lexing.network
Slovaquie <i>Slovakia</i>	Rowan Legal	Michal Nulicek Josef Donat	+420 224 216 212	slovakia@lexing.network
Suède <i>Sweden</i>	Eris Law Advokatbyrå	Katarina Bohm Hallkvist	+46 (0) 70 646 6768	sweden@lexing.network
Suisse <i>Switzerland</i>	Lexing Switzerland	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier Diffusée uniquement par voie électronique – gratuit- ISSN 1634-0701

Abonnement à partir du site : <https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/>

©Alain Bensoussan 2022 — Crédit photo/Photo credits : <https://www.alain-bensoussan.com/notice-legale/credit-photo/>