China and WTO Review (CWR)
2024, 10(1), 87-100
ISSN: 2384-4388
https://cwto.net

Research Article

Toward a Comprehensive Cyber Law Framework: Assessing Avatar Legal Liability

Sayid Muhammad Rifki Noval [1*], Irma Rachmawati Maaruf [2]

[1] Professor, Department of Law, Universitas Pasundan, Bandung, Indonesia
[2] Lecturer, Department of Law, Universitas Pasundan, Bandung, Indonesia
* **Corresponding Author:** Sayidrifqi@unpas.ac.id

Citation: Noval, S. M. R., & Maaruf, I. R. (2024). Toward a comprehensive cyber law framework: Assessing avatar legal liability. *China and WTO Review, 10*(1), 87-100. https://doi.org/10.52152/cwr.2024.10.1.07

ARTICLE INFO

Received: 23 Jul 2024
Accepted: 24 Oct 2024

ABSTRACT

Enforcing the right to security on the internet remains a never-ending task. The problem becomes more complex when the metaverse creates a new dimension for internet users to interact, including the use of avatars. However, this novelty has taken its toll, with a series of events experienced and committed by avatars in the metaverse. The current law has not been able to provide legal certainty, whether avatars can be held responsible for their actions, and how law enforcement is against avatar users. This paper seeks to shorten that distance, by suggesting that the concept of virtual identity or digital passport should be mandatory, in order to identify the real person behind the avatar. Furthermore, it recognises the avatar as a legal subject, using the concept of corporate law, so that the user behind the avatar can be held legally responsible for their actions in the metaverse.

Keywords: Avatar, Cyber Law, Cyber Sexual Harassment, Metaverse.

INTRODUCTION

The debate on the presence of law in cyberspace has yet to find a full consensus, given the presence of freedom advocates in cyberspace who seem to be against any regulation or limitations imposed through legal instruments. When the researchers are trying to shorten the distance of the tension, the presence of the metaverse again fills the next queue of homework that needs to be addressed immediately. The general reasoning of the opponents is based on the view that the benefits offered by the free and unregulated exchange of ideas far outweigh the dangers, and that freedom is what characterises cyberspace. The perspective sometimes referred to as cyberspace idealism posits that cyberspace represents a utopian domain of the intellect, whereby individuals can engage on an equal footing, liberated from the limitations imposed by societal, historical, and physical factors. Cyberspace idealism often results in conflicting reports on the issue of cyberspace reality. One perspective suggests that cyberspace is frequently regarded as possessing a greater sense of reality compared to physical existence. Conversely, offences perpetrated in the realm of cyberspace are frequently regarded as lacking tangible reality, given their non-physical nature and absence of direct bodily harm. One frequently cited instance is the notion that the preservation of freedom of speech inside the realm of internet is indeed tangible and warrants robust safeguarding. However, cyber harassment is not real, so it is often not taken too seriously (Franks, 2011).

The discussion of virtual sexual assault or harassment has actually been elaborated very well by John Dahaner in his article entitled The Law and Ethics of Virtual Sexual Assault. Dahaner commences by citing Litska Strikwerda's perspective, which posits that the concept of "virtual sexual assault" can be classified as a subset of "virtual acts". The concept of virtual action refers to any action initiated by a user within a virtual environment, encompassing both objects and individuals present within this environment. Virtual sexual assault can be described as the occurrence of sexually explicit behaviour between virtual characters within a virtual environment, wherein such behaviour is performed without consent, is coerced, or is unwelcome (Barfield & Blitz, 2018). The occurrence of online harassment within the metaverse is not a recent phenomenon. According to a recent study conducted by the Pew Research Centre, it was revealed that a significant proportion of the United States adult

population, specifically 41%, has reported firsthand encounters with various manifestations of online harassment. This finding indicates a notable escalation in the prevalence of such incidents when compared to data from 2017 (Vogels, 2021). Mikaela Jade, CEO of Indigital, a technology education company, shares her experience as a holographic avatar. She once found out that another avatar was placing his head under her avatar's "crotch" (Broad, 2021). However, it is important to note that most of the current regulations are ineffective in cracking down on sexual harassment, one of the main reasons being that the perpetrator's behaviour or actions do not fall under or can be properly captured by the categories of defamation, threats, invasion of privacy let alone sexual harassment (Franks, 2011).

Another case occurred in 2016 Jordan Belamire, a player of the VR video game QuiVr, described his experience of being groped in the game. Belamire wrote that someone approached him and rubbed something against his chest (McDougall, 2022). A report written on Gawker Media under the title "Second Life: Rape for Sale" also revealed how Second Life users apparently indulge in rape fantasies. This is based on a rape that occurred on a virtual beach after another avatar invited her to swim (Avatar Rape, 2010). Further research was conducted by the SumOfUs organisation, which has now morphed into Eko. In 2022, SumOfUs released a report entitled Metaverse: another cesspool of toxic content that revealed the dark side of the metaverse. The research team that entered Horizon Worlds had a similar experience, with sexual harassment being an immediate response. Approximately one hour subsequent to using the platform, a researcher affiliated with SumOfUs was escorted to an exclusive area within a social gathering, where they were subjected to sexual assault perpetrated by other individuals. The individuals involved consistently instructed her to face the opposite direction, so subjecting her to harassment from behind. Other users in the room were seen witnessing the act by passing around bottles of liquor. Another researcher at Horizon World had a similar experience, where her avatar was harassed by being groped by another avatar. Meanwhile, researchers at Population One reported that an avatar simulated groping and ejaculation on his avatar, and his colleague wearing a haptic vest had her breasts groped by another avatar and in late 2021, one of Meta's internal company testers reported being sexually harassed in Horizon World. Her avatar had been groped by another avatar (Basu, 2021).

In 2015 the UN Human Rights Council adopted a landmark resolution recognising digital rights by asserting that "the same rights that people have offline must also be protected online, including the right to privacy" (Noval, Soecipto, & Jamaludin, 2022). With this recognition, three digital rights were born that received special attention, namely: (1) right to access; (2) right to express; and especially (3) right to online safety, which includes the protection of the presence of a sense of security from sexual violence in cyberspace (Noval, 2021). This is one of the moments to argue and strengthen protection for internet users, so that internet users should be able to obtain legal protection when using the internet, even through avatar representations, including from sexual harassment in the metaverse.

Avatars are a new representation of the user in the metaverse, and serve as the user's digital identity in the virtual space. Avatars in the metaverse are able to represent users' different moods, tastes, and appearances, and ultimately shape the way users interact in the metaverse. According to a survey published by Virtua, there exists a significant desire among the younger demographic in the prospect of redefining their identities inside a virtual realm, wherein the establishment of digital personas and ownership is made possible. The study revealed that a significant proportion of American millennials, specifically 63%, hold the belief that the Metaverse will play a pivotal role in facilitating their personal transformation. Additionally, a substantial 70% of the studied American population expressed agreement with the notion that digital commodities, including apparel and artwork, currently hold considerable significance in shaping their individual identities. A study conducted by Microsoft in 2022, encompassing a sample size of 31,000 individuals across 31 nations, revealed that 52% of employees exhibit a willingness to engage with digital immersive spaces within the metaverse for the purpose of conducting meetings or participating in team activities within the upcoming year. Furthermore, 51% of individuals belonging to Generation Z and 48% of Millennials envision incorporating elements of their professional responsibilities within the metaverse within the subsequent two years. The metaverse has been recognised as a significant advancement towards fostering a sense of togetherness among individuals, despite their physical separation (Microsoft Team, 2022). Tout argues that cyberspace, including the metaverse, relies heavily on the transfer of identity from the real world to cyberspace. It is this process of translation that contains a degree of skeumorphism - the preservation of familiar traits - in redesigning the self. The introduction of avatars in Second Life has led to interpersonal relationships that inherently change what has been established on the internet (Howatson-Tout, 2022). According to futurist Ray Kurzweil, the convergence of technology and human beings is referred to as the "singularity," denoting a state in which the distinction between the two entities ceases to exist. In the documentary released in 2010, which serves as a companion to his book titled "The Singularity is Near," Kurzweil introduces a fictional character named Ramona. Ramona, an avatar, engages the services of Alan Dershowitz, a civil liberties lawyer, to advocate for the legal acknowledgment of her personhood as a conscious entity. This

pursuit takes place within a speculative future context characterised by "fleshism," a discriminatory ideology that marginalises individuals of virtual origin (Buchleitner, 2021).

Individuals who engage with the metaverse, predominantly through the utilisation of virtual reality (VR) technology, are inclined to select an avatar as a means of self-representation. The avatar's motions and actions will be coordinated with the user's own movements and gestures, facilitated by the tracking of their head and hands through the virtual reality (VR) headset and controllers. The user assumes the role of an embodied puppeteer, so experiences a first-person perspective within the virtual world. Avatars have the ability to navigate the metaverse realm without constraints, while users typically engage in real-time dialogue with fellow avatars through the audio communication technology integrated within their respective headsets (Vorderman, Allen, & McIntosh, 2022). The growing use and efficacy of metaverse technology imply that the worth of digital identities will escalate. As the fidelity and durability of the user's virtual embodiment in the metaverse increase, there arises a prospect of faithfully replicating the user's physical look. The utilisation of several technologies for interaction inside the Metaverse, including sensors, eye tracking, face tracking, and haptics, is widely acknowledged (Europol, 2022). VR technology has obliterated the gap between physical and digital selves, creating immersive experiences that enhance realism and emotional connection. Users can watch as digitally rendered hands grope representations of their own bodies, and it all feels increasingly real. And it's this, which is taking serious note, especially when it comes to sexual offences in the metaverse. Researchers at Carnegie Mellon University have developed a VR add-on for headsets that can deliver ultrasound waves to the mouth, allowing users to feel sensations in the lips and teeth. With the add-on, users can feel the touch of spiders, raindrops, and even the flow of a water fountain on their lips. Users can simulate the activity of brushing their teeth (McDougall, 2022). Another development is by VR Bangers who have launched the POV Head Rig, a disembodied mannequin head with a camera for the eyes that will help make VR porn more intimate and emotional (Cole, 2017).

In 2010, Orin S. Kerr expressed his concern about technological developments in the legal world, particularly in the area of criminal law. The individual's apprehension revolved around a pair of inquiries, specifically: "At what point does the conduct of individuals participating in virtual world games online give rise to accountability for criminal acts in the physical realm?" and "Will forthcoming criminal legislation necessitate addressing novel societal detriments arising in the realm of cyberspace?" Kerr disclosed that during that period, the legal regulations pertaining to cyberspace exhibited minimal or negligible consideration towards virtual reality. In the realm of criminal law, there is a prevailing tendency to prioritise the regulation and enforcement of tangible entities above their virtual counterparts. The legal system places greater emphasis on the actions of an individual rather than the subjective experiences of the victim. The aforementioned phenomenon significantly restricts the scope of criminal legislation inside the realm of online. The current legal framework does not encompass the recognition of virtual murder, virtual threats, or virtual theft. Although these "offences" may seem like cyber counterparts to conventional crimes, the current legal framework necessitates tangible evidence rather than virtual comparisons. The physical perspective diminishes the significance of criminal law within the realm of online. Virtual worlds are subject to regulation similar to conventional games, however, their virtual nature typically does not hold legal significance outside the context of criminal law (Kerr, 2008).

In contemporary criminal law, an individual is deemed to have committed a specific offence when all the requisite parts of the crime have been satisfied. Nevertheless, contemporary crimes predominantly encompass physical aspects, necessitating tangible actions, communication across physical locations, and affecting individuals in a physical manner. An illustrative instance is the criminal offence of prohibiting murder, as it entails the deliberate termination of an individual's life, rather than the demise of a virtual representation. The commission of an infraction necessitates the actual presence of an individual within a designated area, as opposed to any form of virtual presence. The primary effect of adopting the physical approach is that the majority of internal offences occurring in cyberspace would not be considered criminal acts according to traditional physical criminal law. As an illustration, one virtual representation, commonly referred to as an avatar, illicitly appropriates important information from another avatar. Can this be classified as an act of theft? While some users may hold such a belief, it is important to note that the legal framework generally does not align with this impression. The rationale behind this perspective is that the act of "virtual theft" is frequently regarded as an inherent aspect of the game's regulations. There exists a perspective positing that virtual worlds can be classified as games, as participants willingly engage in their participation, motivated by either recreational enjoyment or potential financial gains, like other conventional games. Similar to other games, virtual world games possess artificial regulations that dictate the actions and limitations of participants. Hence, if an action that may seem like "theft" within the virtual realm aligns with the established rules of the game, it cannot be considered theft under the purview of criminal law when examined from a physical standpoint. According to the observations made by Dan Hunter and Greg Lastowka, game norms serve as substitutes for the conventional rules that govern society (Kerr, 2008). Tiffany uses the basis of a well-known legal maxim, Volenti non fit injuria (There is no injury to one

who consents). An example is given of a sports match, to show why cyberspace cannot allow tort claims. The maxim "there is no injury to one who consents" is why a football player cannot sue another player who makes a "tackle" during a match, even if the "tackle" results in a lasting and permanent injury or the tackle is considered an offence (Day, 2009).

But of course, a series of sexual harassment incidents against and by avatars in this metaverse cannot be viewed as a game, because the serious impact it causes even injures the right to security of internet users, so legal instruments must be present to provide legal protection. James Lemon, a 36-year-old man who experienced harassment during his Echo VR activities, stated that verbal abuse and racism in virtual reality do not feel different from similar intimidation in the real world (Wong, 2021). A research investigation conducted on participants engaged in the online game "Lineage" substantiates the notion that virtual acts of violence possess the capacity to elicit noteworthy emotional repercussions among those affected. The study also unveiled that experiencing violence is not indicative of obsessive or aberrant behaviour, but rather a prevalent occurrence among individuals who are emotionally invested in online activities. The emotional involvement exhibited by individuals facilitated their enjoyment and satisfaction in engaging with online communities. However, this emotional investment also rendered them susceptible to the potential negative consequences of virtual injury (Wolfendale, 2007). It is interesting that many findings reveal that virtual world interactions have a certain positive impact on users, recognising that the influence can trigger happiness, but on the other hand not recognising the potential harm that can be received by other users, such as in the case of virtual sexual harassment.

Several individuals who experienced sexual harassment in the metaverse expressed their determination to never tolerate such disrespectful communication in the future. The phenomenon of identifying with the avatar entails perceiving injury inflicted on the avatar as harm inflicted upon the individual. This paper examines the phenomenon of avatar attachment and highlights the enhanced character-controller identification experienced in virtual environments as a result of the incorporation of quasi-physical presence. The prevalence of connection to avatars and the consequential grief caused by damage to avatars can be attributed to the interplay between presence, identity, and communication (Wolfendale, 2007). This paper does not provide a perfect concept, but seeks to shorten the distance in law enforcement efforts against perpetrators of sexual harassment. Therefore, this paper is limited to providing a basis for argumentation to ensure the identification of the avatar user to the recognition of the avatar as a legal subject.

METHODOLOGY

The research method used is normative juridical with a statute approach, case approach, analytical approach, and comparative approach. The data used in this research is secondary data. Secondary data collection is done through a literature study. Legal materials used are primary and secondary legal materials. Data analysis is done descriptively and qualitatively. The specification of this research uses an analytical description.

RESULTS AND DISCUSSION

Avatar and User Identity

The tension in the recognition of the fading boundary between the virtual and the real world, inserts a serious problem of legal liability for actions that are considered to have harmed internet users when doing activities in cyberspace. The internet indeed presents a new experience in a pleasant way, with its main features referred to as the Triple A Engine, namely easily accessible, affordable, and anonymous (Koops, Dekker, & Briken, 2018). The ability of cyberspace idealism to garner a significant following, particularly among persons who perceive their life experiences as constrained by factors such as physical identity, social standing, age, gender, or physical appearance, is to be expected. Through engaging in online activities, individuals have the opportunity to encounter a form of positive anonymity. In the realm of cyberspace, individuals have the option to withhold their race, gender, and actual age, so enabling them to evade the detrimental stereotypes associated with these characteristics. This online environment offers a unique opportunity, particularly for historically marginalized communities, to circumvent the negative repercussions that they may encounter in physical reality (Franks, 2011).

The concept of cyberspace idealism needs to be viewed carefully, without obscuring the horrific facts that have occurred to date. Cyberspace needs to be seen in another light, that of an unauthorised state, where certain powerful groups oppress, threaten and harass those who are not powerful. This is close to the view of John Locke, who saw an unauthorised state as one in which some groups take liberties at the expense of others. Locke argued that such a state is no longer "natural", requiring legal intervention (Franks, 2011).

Supporters of cyber freedom consider that what happens in cyberspace will and must follow the prevalence of regulations that specifically apply in their world, without being intervened by anything including the rule of law that applies in the real world. While it is known, that situation can certainly trigger the birth of problems for internet users. The current legal system ensures that legal responsibility can only be carried out when the identification of the perpetrator can be carried out, and these conditions tend to be easy to do in the real world, but complications will soon be faced when the virtual world makes it easy for users to cover the veil of their identity, which is then known as anonymous.

This anonymity is certainly not entirely correct when applied absolutely. There are at least two (2) arguments that need to be considered. Firstly, a lesson can be learnt from the story of the ring written by Plato in his work The Republican. A shepherd, named Gyges, accidentally found a cave, with a skull wearing a ring on its finger. The ring turns out to have the ability to make its user invisible and certainly anonymous. With the power of the ring, Gyges seduced the king's wife and tried to kill the king to take control of the kingdom. The power even made Gyges free from the restrictions of custom and reputation, able to steal whatever he wanted, have sex with whomever he chose, kill or release from prison whomever he wanted, and never get caught (Kim & Julian, 2007). In his writings, Plato then posed the question, will those who wear the ring be polite and moral? According to him, no, and the internet has proven Plato's assumption to be correct (Isaacson, 2016). Users of the Gyges ring can act immorally simply because they know that they will not be caught and identified. A study conducted by Ruogu Kang revealed that 53% of anonymous internet users have admitted to having committed various criminal activities, such as hacking or harassing other internet users (Kang, Brown, & Kiesler, 2013). This condition makes anonymity a trigger and even results in reduced legal certainty (Dodge, 2021).

The second argument is based on the strong falsity in cyberspace since ancient times. Spooner employs the concept of manipulation. In his research focused on virtual games, Spooner delineates four overarching user typologies distinguished by distinct motives for engagement, namely: achievers, explorers, socialisers, and murderers. Achievers have a strong drive to accomplish objectives and emerge victorious in the game, whilst explorers engage in boundary-testing activities inside the game environment and embark on exploratory quests. Socialisers actively engage in various social groups and cultivate interpersonal connections with fellow users. Lastly, killers actively seek strategies to assert dominance over other users. A recent study has been conducted, which classifies users into five distinct categories, namely relationships, manipulation, immersion, escapism, and achievement (Spooner, 2012).

From the above categories, it can be seen that there are user motivations for activities in virtual spaces that are based on intentions to deceive, manipulate, lie and falsify. So, it is inevitable that there is an urgency for an active response to protect other users from this group. The problems that potentially arise from this manipulation will be very diverse. Parks revealed the dangers of avatar fakes that can influence others. According to the individual's perspective, the credibility and relevance of messages to the intended audience are enhanced when the source is perceived as someone respected or possessing similarities with the audience. Hence, the dissemination of information via established, reliable, and esteemed channels constitutes a crucial step in the process of delivering messages (Parks, Cruz, & Ahn, 2014). This certainly needs to be anticipated, because there have been many figures who have created their virtual identities in cyberspace in the form of avatars, making it possible to send messages that are not true and are received by other users. From these two arguments, it can be seen that anonymity can actually become a time bomb on the internet, when there are no rules in its application. So, it is necessary to consider the presence of policies that can ensure the true identity of internet users, either in the form of digital identities, registration mechanisms for avatars, or restrictions on revealing one's identity when needed in legal processes.

The World Economic Forum (WEF) has conducted an in-depth study on digital identity, which has become one of the problems of today's virtual world. According to him, currently most internet users do not have their own digital identity, but rely on applications such as Facebook, Google, or LinkedIn to authenticate or log in. The capacity to transfer authentication does not provide a digital identity that is possessed, administered, and governed by the individuals who possess the information and identity. Instead, it remains a component of another entity's data monetization initiative. In order for individuals to assert ownership over their digital identities, it is imperative to establish and enforce standardized protocols that facilitate their recognition and authentication across various contexts (Bonner, 2022).

The World Economic Forum (WEF) subsequently proposes a solution to tackle this issue, which involves the implementation of digital identities that are linked to pre-existing physical identities. One potential scenario entails the inclusion of established authentication methods, akin to an individual's identity in the physical realm, within a user's digital identity. These methods may encompass various forms of identification, such as a driver's license, national insurance or social security number, passport, or biometric data like retina and fingerprint

information for individuals. Similarly, companies could rely on identifiers such as a company number or operating license to establish their digital identities. This concept has the potential to function as an artifact or indicator within a comprehensive digital identity, symbolizing a manifestation of credibility, comparable to an endorsement in a travel document. According to the World Economic Forum (WEF), it is anticipated that in the forthcoming years, an individual's digital identity will no longer be a solitary entity, but rather a distinctive central component related to numerous other digital entities. This will give rise to a very intricate and interlinked network of information strands. The phenomenon of data fragility may have a significant impact in this particular scenario, particularly when the removal or alteration of data within a singular record or system results in a potentially extensive proliferation of data inconsistencies and disrupted linkages among the interconnected data strands. Hence, it is imperative to incorporate resilience into the digital identity architecture from its inception in order to effectively address these unavoidable occurrences (Bonner, 2022).

In line with the WEF's view on digital identity, other scholars have come up with an alternative concept that has become known as the "digital passport". With this passport, users will act with a single digital identity, which can be used to identify themselves and carry information across various metaverse platforms. Union ID is one example of a digital passport released by Union Avatar. With Union ID, a user's identity is all in one place. No more split identities across networks. Users can have it and can carry it, almost anywhere. Interoperability between third parties and the platform, allows users to carry their assets with them and have full control over how they are used and which data is shared with third parties (Union Avatars, 2023).

It is known that a group of experts consider that virtual identity will face conceptual challenges, because it is basically something different from the concept of identity in cyberspace. Virtual identity is a new phenomenon that has its own architecture and is different from the real world, so it certainly requires new legal concepts. Nevertheless, it is imperative to acknowledge that a user's virtual identity serves as a social representation within the online realm, affording the user a notable level of agency in shaping their identity, distinct from their offline existence. Therefore, Naseh agrees with the concept of legal recognition of virtual identity, which can only be officially granted by legislation to each individual based on certain rules, which is termed a legally virtual personality (Naseh, 2016).

The intersection of digital identity and the internet is nothing new, as it is in the realm of pornography. As early as 2023, Louisiana had stipulated that every internet user who would access pornographic content would be required to show a "digitised identification card" to confirm the age of the user. Currently, seven more states are following suit, including Arkansas (Cole, 2017). However, there are concerns that this concept would mean a single global system for establishing digital identities, which would require centralisation, and this is clearly against the principles of the web3. Not only that, it would also limit choice and allow centralised organisations to track user data, something that has become a sensitive issue in cyberspace. The counterbalance to this concept is to have a decentralised identity system distributed among different organisations. This avoids the problem of centralisation, although it is a major challenge to ensure that all organisations follow suit (Siejca, 2023). Caution in this concept is necessary considering that efforts to use real user data have caused controversy. In 2011, Facebook imposed a requirement to use real names in cyberspace under the pretext of reducing cyberbullying. Mark Zuckerberg wanted "anonymity gone". Not only that, this policy will force people to behave better (Opsahl & Rodriguez, 2021).

An interesting alternative view is Lutatch's concept of virtual identity. According to him, identity in the metaverse should be considered authentic from the start. The disclosure of David Lucatch's real-life identity is not a prerequisite for other users to recognize his virtual character within the metaverse. It is imperative for other users to be aware that the persona in question is substantiated by the authentic identification of an actual individual. The focus lies not on the disclosure of one's identity, but rather on the provision of access exclusively to individuals who have been authenticated as genuine. The topic under consideration pertains to the implementation of measures aimed at ensuring safety, security, and privacy restrictions. The evolution of human relationships within the metaverse parallels that of the real world, necessitating a comprehensive understanding of the individuals with whom we engage, as is similarly crucial in offline environments. The utilization of a verified digital identity provides individuals with the assurance that they are engaging with genuine individuals within the realm of cyberspace. The implementation of mechanisms to authenticate the identification of individuals mitigates the prevalence of fraudulent activities and identity-related concerns that are inherent in online interactions (Lucatch, 2021). With this concept, the anonymity that is often an advantage of cyberspace can still be present. A person can still use a name, avatar shape and other characteristics that are different from the original, but when involved in a business transaction or violation of the law, there is an entity that can inform the original identity of the avatar, so that it can hold it legally responsible.

Australia is a pioneering example that has approached the concept of digital identity, though not quite in the

same way. Since June 2023, the identity programme in Australia has been under the authority of the Department of Finance. Australia explains that digital identity is a safe, secure and convenient way to prove one's identity online, to access government online services. Digital identity, allows users to prove themselves online for work, education and personal use, and can reuse their digital identity whenever needed (Australian Government: Digital Transformation Agency, 2023).

In Seguin's view, in the case of defamation committed by an avatar to another avatar, the court should not be able to dismiss the case on the basis that it was committed by the avatar. According to him, there have been various cases in the English courts that can be considered, such as cases of disputes over property rights in the real world on the Second Life platform, as well as defamation cases relating to the liability of internet site owners. Furthermore, Mr Seguin gave his views on the status of avatars that judges need to consider when a case arises. There are three categories, namely avatars as public figures, limited purpose public figures, or private figures. These three categories can be the first step in determining whether or not an avatar is legally liable (Seguin, 2010). Recalling Lastowkan and Hunter's view that avatars functioning in virtual worlds are cyborgs, or "technological extensions of the self," where users communicate with others in virtual spaces through computerised self-representations, the analogy is that of a scientifically sophisticated "prosthetic leg" (Lastowka & Hunter, 2017). Therefore, the Avatar cannot be considered a free entity whose activities can avoid regulations and even morals that exist in the real world.

Why is it important to ascertain the owner of the avatar, because ultimately the closest step in providing protection and enforcement, is to ensure that the law can identify the person behind the artificial entity and reach them. Basically sanctioning the actual person behind the fictional form has been recognised in various legal systems. For example, the 1920 US-UK Arbitration Tribunal established that in the event of a legally exceptional circumstance, it is necessary to refer to widely acknowledged principles of fairness and fair treatment in order to ascertain the rights of the individuals concerned. The courts have consistently applied the principle of fairness in cases where recognizing the legal personality of a company would result in an unjust outcome or go against the intent of the law. This principle can also be applied in similar situations. In instances of this nature, judicial bodies have demonstrated a willingness to delve beyond the legal construct and examine the human persons who ultimately reap the benefits (Bryson, Diamantis, & Grant, 2017).

With the identification of a person, the real human behind his virtual identity, the law enforcement process can continue with the certainty of the availability of the suspect, who is held accountable for his actions or deeds, either directly or through the intermediary of an avatar in the virtual world. However, this homework is not finished, considering that the identification of the person does not necessarily make him legally liable. Therefore, efforts are needed to take the next step to ensure that the virtual entity is a legal subject.

Concept of Company Law

The next issue related to harassment that occurs in the virtual world, is to ensure the responsibility of the person behind the avatar when allegedly committing acts of sexual harassment in the metaverse. Hence, holding that person legally responsible requires the right regulation, which recognises the avatar as a legal subject. Psychologist John Suler has identified a phenomenon known as "toxic disinhibition" in the realm of online interactions. This refers to the inclination of individuals to deviate from established social standards in contexts that afford anonymity or the ability to assume alternate identities, such as through the use of avatars. Avatars provide users with the opportunity to dissociate from their authentic identities, enabling them to engage in behaviors that diverge from their real-life personas. The utilisation of this technology enables the facilitation of communication and behaviour that would otherwise be unachievable within the limitations of face-to-face interactions (Cheong, 2022).

The intellectual origins of the notion of an avatar can be traced back to the sacred tradition of Hinduism. The etymology of the name "Avatar" can be traced back to its Sanskrit root "avatarana," which conveys the concept of progeny. It represents the corporeal manifestation of a divine being or the personification of a transcendent being. The aforementioned concept is commonly associated with Lord Vishnu, who manifested on earth in ten distinct forms known as avatars. The purpose of these avatars was to provide human counsel, counteract malevolence, and restore moral order, commonly referred to as Dharma (Buchleitner, 2021). Avatars are used as symbolic representations by individuals who advocate the notion that cyberspace presents a substantial alternative to the tangible world. The presence of certain limitations, such as physical constraints, biases, and divisions, is responsible for this phenomenon. On the contrary, cyberspace offers a domain in which the limitations are only determined by the imaginative and creative abilities of the individual (Franks, 2011).

It is important to note that the term "avatar" functions differently in the context of the physical world compared to its usage in cyberspace. While in the physical world, an avatar represents a tangible embodiment of a superior entity, in the realm of cyberspace, this relationship is inverted. The concept of a higher being can be

understood as the user, while the avatar serves as a digital representation of the user within the realm of cyberspace. The progression of avatar users, transitioning from agents to "surrogates," holds significant significance within the present-day endeavor to advance virtual rights. The integration of avatars into popular usage is intricately connected to the triumph of the computer entertainment sector. Avatars were originally just representative images of users. The rudimentary physical empathy of avatars was seen in the way people swayed, ducked, leaned and even panicked while playing games. As customisation possibilities became more complex, avatars became more of an agent, allowing users to play around with the creation of symbolic avatars and experience different bodies. Developers therefore develop "proprietary feelings" towards their avatars, as users experience what is called symbolic disembodiment, the freedom to be whoever they want and do things that cannot be done in reality (Day, 2009).

The utilization of avatars often fosters toxic conduct, mostly due to the increased probability of impunity. Conventional legal frameworks exhibit limited efficacy in deterring or penalizing instances of racist or hostile conduct on internet platforms. On a global scale, the legal proceedings pertaining to cybercrime in conventional court systems are characterized by a lack of cohesion and clarity, resulting in a complex array of circumstances and potential outcomes. Due to their predominantly territorial jurisdiction, many laws exhibit limited practical relevance when addressing cyber offenses. In the United States, Section 230 of the Communications Decency Act stipulates that "interactive computer services" are immune from being regarded as third-party speakers or publishers of content. Website owners are alone obligated to address significant criminal allegations, such as those pertaining to child pornography or intellectual property infringement (Buchleitner, 2021).

Moderation is often a demand that some experts make in an effort to keep users safe in the metaverse. But according to many specialists, the task of monitoring a vast number of contacts in real time would necessitate substantial exertion and may potentially be unattainable. The shift from checking text, images and videos to watching 3D worlds will be dramatic. In 3D, it is not content that needs to be regulated, but behaviour, necessitating a new type of moderation system. Meta's current plan is to give users the tools to report bad behaviour and block others they don't want to interact with. According to the security film released in 2020 by Horizon Worlds, a virtual reality social game developed by Meta, it has been stated that Meta intends to persist in capturing and documenting activities within the metaverse. However, it is emphasized that this data would be saved exclusively within the user's RV headset. In the event that a user subsequently complains of inappropriate conduct, the recorded video will be forwarded to Facebook's human reviewer for evaluation (Murphy, 2021).

In the empirical realm, a multitude of attachment manifestations exist, each of which is deemed ethically acceptable. The aforementioned circumstance has prompted an inquiry into the extent to which avatar attachment satisfies the criteria for constituting a morally relevant type of attachment, akin to those observed in the physical realm. This inquiry has prompted the perspective that connection to avatars can be perceived as a manifestation of attachment to a fictitious entity. Ultimately, avatars can be regarded as non-tangible entities. These creative inventions are designed for utilization inside fantastical settings, therefore rendering them akin to imaginary companions and fictional entities, rather than tangible objects of emotional connection. Wolfendale holds a contrasting perspective, contending that avatars cannot be equated to either imaginary friends or fictional characters. In contrast to the concept of imaginary pals or fictitious characters, avatars can be understood as active personas assumed by individuals within the realm of cyberspace. The concept of an avatar extends beyond a mere figment of imagination, encompassing a means of online self-expression and the establishment of one's identity. Hence, in contrast to attachment towards an external fictional entity, attachment towards an avatar entails an attachment towards a personally selected and self-fashioned entity. This entity is subject to control, manipulation, and serves as a means for engaging with others. The object in question serves as a representation of an individual within the digital realm, so it does not possess any qualities of imagination. This distinguishes it from imaginary companions or fictitious characters, which are inherently imaginative in nature (Wolfendale, 2007). The concept of representation is what is needed to tie the avatar to the person behind it, and the expansion of the common law subject currently has the opportunity to be given to avatars in the metaverse.

In practical terms, the majority of legal systems acknowledge the existence of two distinct categories of legal entities, namely natural persons and juridical persons. Natural persons are acknowledged only on the basis of their status as human individuals. On the other hand, juridical persons refer to entities that lack human characteristics but are bestowed with specific rights and responsibilities according to legal frameworks. Corporations and several other types of commercial alliances are frequently observed, while there exists a wide range of alternative forms as well. Religious, governmental, and intergovernmental entities possess the capacity to function as legal persons both within national jurisdictions and on the international stage. This demonstrates instances wherein non-human organisms are endowed with distinct personality traits. Additional instances include the temples located throughout India, the rivers found in New Zealand, and the complete ecosystems present in Ecuador. This again shows that a country can attribute personality to a new entity such as an AI system

(Chesterman, 2020). The concept provided by Ben Chester Cheong can be a start to see the possibility of avatars becoming a new legal subject, a concept that offers an adaptive step from the concept of corporate law. Cheong considers that there is a possibility that an avatar can be categorised as a legal subject, in the form of a legal entity. When an avatar possesses the capability to engage in a sequence of actions pertaining to the legal affairs of its users, it becomes imperative to contemplate the implementation of legal personhood inside the metaverse. The legal personhood might be conferred by means of a registration procedure, wherein each individual is eligible for a single avatar inside the decentralized and boundless metaverse (Cheong, 2022).

It needs to be recognised that the debate about avatars in the metaverse is about their recognition as entities that have certain legal legitimacy, which then leads to recognition as a legal subject. Currently, most legal systems tend not to grant legal personality to inanimate objects, and rather grant it to entities that are human in an ethical and metaphysical sense. This may be because most legal systems want to recognise and give effect to the rights and obligations that actual persons have. But this gross generalisation can be misleading. In order to determine whether an entity is a legal person, we have to look at the approach that a particular legal system takes towards such entities as well as the reality of the proliferation of ideas and concepts that have come to exist towards these virtual entities (Bryson et al., 2017).

Cheong's view has received serious support, because he believes that ignoring the presence of avatar rules in the metaverse will have serious consequences, given that the structure of cyberspace allows for the separation between a person's real identity and their virtual identity. Therefore, it is necessary to reject the idea of the requirement of granting legal personality in the metaverse in the form of the presence of conscience of the avatar. According to him, legal personality must exist within the metaverse itself, so that anyone who creates an avatar in the metaverse agrees to subject his or her avatar to the legal personality that will be governed by the laws of the metaverse. The rules should also stipulate that the legal personality, which is separate or distinct from the avatar, will be disregarded if a crime or unlawful act has been committed. Thereafter, the liability of the humans behind the avatars will be determined by the scale of damage caused to both the metaverse community and the real-world community (Cheong, 2022).

Cheong posits that the registration of all avatars within the metaverse should be mandated, drawing a parallel to the process of incorporating a company. There is a compelling argument to broaden the scope of causation and foreseeability under various legal frameworks, such as extending its application to encompass harm resulting from avatars or infrastructure within the metaverse. Companies have the potential to act as a paradigm for the expansion of rights to avatars within the metaverse. Similar to corporations, avatars are non-human entities that serve the purpose of enhancing economic investment within the market. While individuals in society are bound by rights and responsibilities, corporate law has constructed a mechanism called a legally personified corporation, which is distinct from a private individual. A significant distinction between businesses and robots lies in the fact that corporations invariably operate through human agents, with ultimate decision-making authority still vested in humans. Likewise, within the context of an avatar, agency is mediated by human operators, with the ultimate decision-making authority being in the individual controlling the avatar. This bears a resemblance to a corporate entity in that it is required to operate through an individual agent. A corporation can incur liability in a manner analogous to that of an individual for both criminal offenses and civil wrongs. Nevertheless, there exist constraints when imposing penalties on a corporation, as it is not an individual entity (Cheong, 2022).

The integration of avatars can be implemented in a manner analogous to the establishment of entities in accordance with business legislation, wherein a registration number is assigned. The registration data of the avatar's ultimate owner, whether an individual or a corporate entity, will be recorded in a metaverse register. In the case of a company, a quick search through the official state information system can reveal the controller behind the company. But there exists a perspective suggesting that, when it comes to avatars, there should be a degree of variability regarding the disclosure of the avatar's identity as a fundamental entitlement. In the event that individual operates an avatar and deliberately refrains from disclosing their genuine identity, it is appropriate to acknowledge their anonymity unless a significant violation of the law has occurred (Cheong, 2022).

Similar to Cheong, Chestermen also uses the concept of corporate law in looking at virtual entities, such as Artificial Intelligence (AI). According to the individual in question, there exist two primary justifications for considering artificial intelligence as a legal entity. Firstly, the establishment of a party to assign responsibility in the event of an adverse outcome. Furthermore, it is imperative to establish a mechanism that guarantees the presence of an individual who may be duly acknowledged and compensated in the event of favorable outcomes. Chestermen eventually tried to find reasons that personhood could be granted, either instrumental or inherent reasons. The instrumental reason is based on the concept of a legal entity that has been commonly used, namely a corporation. However, another reason is that if an AI system has reached the point of being indistinguishable from humans, such as passing the Turing test, then it is entitled to a status comparable to humans. A frequently

cited example is the robot Sophia who was granted citizenship by Saudi Arabia in 2017 (Chesterman, 2020). In addition to Sophia, Shibuya Mirai is another notable chatbot that has garnered attention. Programmed to emulate a seven-year-old kid, Shibuya Mirai holds the distinction of being the first AI bot to receive official residency status in Tokyo, Japan. This unique designation enables Shibuya Mirai to serve as an official resident, with the primary purpose of actively engaging with and soliciting the viewpoints of Shibuya inhabitants (Cuthberston, 2017). Another illustration can be observed in the case of Deep Knowledge Ventures (DKV), a firm that specializes in the development of pharmaceuticals for age-related diseases and regenerative medicine initiatives. DKV made the decision to include a computer program named Vital as a member of its board of directors. Vital possesses the capacity to provide investment suggestions pertaining to life science enterprises through the meticulous analysis of extensive datasets. The Validating Investment Tool for Advancing Life Sciences (Vital) has proven crucial in facilitating the board's decision-making process, enabling more rational and informed choices. Moreover, Vital has played a pivotal role in rescuing the company from a state of imminent financial collapse (Burridge, 2017).

When the identity of the user is finally known, and the avatar is recognised as a legal subject. Then there is an opportunity to enforce the law against criminals in the metaverse. One of the supporters of this view is Tiffany, who believes that there are opportunities for criminal law to be provided in interactions in virtual worlds involving avatars, such as in cases of defamation. As to her assertion, the emergence of defamation claims in virtual worlds or games can be attributed to the existence of a recognized association between an avatar and an individual in real life. When there is an inherent connection between an avatar and the individual operating the corresponding account, it can be argued that the reputation of the avatar is adequately associated with the account owner, hence allowing for assertions to be made regarding comments made by the avatar. From this standpoint, one can draw a parallel between the association of the avatar and the user and the connection between an inanimate corporate entity and a sole shareholder. In this scenario, the entity effectively represents the controller's 'alter ego', so enabling actions to be justifiably undertaken (Day, 2009). An alternative perspective is articulated by Brenner (2008). According to the author, the current state of criminal law can be attributed to a lengthy accumulation of knowledge and practical application over numerous centuries. Throughout history, the physical realm has been seen as the sole inhabitable domain, hence serving as the exclusive arena for individuals to engage in harmful actions towards others or their possessions. Consequently, it became imperative for the criminal justice system to adapt in order to effectively address instances of tangible bodily injury. While the criminal law has progressively broadened its jurisdiction to encompass certain forms of "soft harms" associated with moral damage in recent decades, its fundamental foundations remain rooted in tangible injury. The contemporary human sphere of activity extends beyond the confines of the physical world. The emergence of cyberspace has introduced a novel realm devoid of physical boundaries, wherein individuals are able to engage in a wide range of activities, potentially encompassing all those conducted in the tangible world. The introduction of this novel paradigm in human endeavors has diverse implications for the field of criminal law (Brenner, 2008).

Brenner vehemently refutes the perspective positing that crimes committed within virtual realms are confined solely to the virtual domain, so presupposing that the resulting harm is likewise limited to the virtual realm. According to Brenner, the act of engaging in criminal behavior within a virtual world cannot be exclusively confined to the virtual environment. The individuals responsible for committing acts and those who experience harm are situated within the physical realm, which serves as the focal point for specific consequences within the virtual realm. The actions associated with engaging in criminal activities within virtual environments are, to a certain extent, manifested within the virtual realm, yet fundamentally remain rooted in the physical world (Brenner, 2008).

CONCLUSION

Efforts to provide legal protection for internet users, especially for crimes committed by avatars and against avatars in the metaverse can be done by ensuring the identity of the perpetrator and his position to be legally responsible. Regulations that force avatar owners to reveal their true identity can consider the concept of virtual identity, digital passports and even identity verification that can only be revealed in the context of law enforcement. The next step is to recognise an avatar as a new legal subject by applying the concept of company law, which requires a registration process. Countries can look at New Zealand and India's move to recognise rivers as legal subjects, to Saudi Arabia granting citizenship to a robot.

ACKNOWLEDGMENT

Thank you to the Ministry of Education, Culture, Research and Technology of the Republic of Indonesia for

funding the research team for the 2023 period, until finally making the material for writing this paper.

REFERENCES

Australian Government: Digital Transformation Agency. (2023). *Digital identity*. Retrieved from Australian Government: Digital Transformation Agency website: https://www.dta.gov.au/our-projects/digital-identity

Avatar Rape. (2010, February). *Inside Higher Ed*. Retrieved from https://www.insidehighered.com/views/2010/02/25/avatar-rape

Barfield, W., & Blitz, M. J. (2018). *Research handbook on the law of virtual and augmented reality*. Cheltenham, UK: Edward Elgar Publishing.

Basu, T. (2021, December). The metaverse has a groping problem already. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/

Bonner, M. (2022). *Why we need to regulate digital identity in the metaverse*. Retrieved from World Economic Forum website: https://www.weforum.org/agenda/2022/12/digital-identity-metaverse-why-we-need-to-regulate-it-and-how/

Brenner, S. W. (2008). Fantasy crime: The role of criminal law in virtual worlds. *Vanderbilt Journal of Entertainment and Technology Law*, *11*, 1.

Broad, E. (2021). Will women be safe in the next stages of the metaverse?. *Bazaar*. Retrieved from https://harpersbazaar.com.au/virtual-sexual-harassment-in-the-metaverse/

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*, 273–291. doi:10.1007/s10506-017-9214-9

Buchleitner, J. (2021, March 18). Rise of the clones: Even our avatars suffer real-world prejudices. *L'Atelier*. Retrieved from https://atelier.net/insights/avatars-and-racism

Burridge, N. (2017). Artificial intelligence gets a seat in the boardroom. Hong Kong venture capitalist sees AI running Asian companies within 5 years. *Nikkei Asia*, *10*. Retrieved from https://asia.nikkei.com/Business/Artificial-intelligence-gets-a-seat-in-the-boardroom

Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity Law Review*, *3*(2), 467–494.

Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly*, *69*(4), 819–844. Retrieved from https://ssrn.com/abstract=3682372

Cole, S. (2017, January 31). This horrific mannequin head camera wants to make VR porn more intimate. *Vice*. Retrieved from https://www.vice.com/en/article/d7x3yw/mannequin-head-camera-vr-porn

Cuthberston, A. (2017, November 6). Tokyo: Artificial intelligence 'boy' Shibuya Mirai becomes world's first AI bot to be granted residency. *News Week*. Retrieved from https://www.newsweek.com/tokyo-residency-artificial-intelligence-boy-shibuya-mirai-702382

Day, T. (2009). Avatar rights in a constitutionless world. *Hastings Communications and Entertainment Law Journal*, *32*, 137. Retrieved from https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol32/iss1/5

Dodge, C. E. (2021). *The ring of Gyges 2.0: How anonymity providing behaviors affect willingness to participate in online deviance* (Doctoral dissertation, University of South Florida). Retrieved from https://www.proquest.com/openview/64d37b9d07960686810a7e9c282e8ab8/1?pq-origsite=gscholar&cbl=18750&diss=y

Europol. (2022). *Policing in the metaverse – What law enforcement needs to know – An observatory report from the Europol innovation lab*. doi:doi/10.2813/81062

Franks, M. A. (2011). Unwilling avatars: Idealism and discrimination in cyberspace. *Columbia Journal of Gender and Law*, *20*, 224.

Howatson-Tout, K. (2022, November). The art of the profile picture portrait. *Right Click Save*. Retrieved from https://www.rightclicksave.com/article/the-art-of-the-profile-picture-portrait

Isaacson, W. (2016, December). How to fix the Internet: Anonymity has poisoned online life. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2016/12/how-to-fix-the-internet/510797/

Kang, R., Brown, S., & Kiesler, S. (2013). Why do people seek anonymity on the internet? Informing policy and design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2657–2666. doi:10.1145/2470654.2481368

Kerr, O. S. (2008). Criminal law in virtual worlds. *The University of Chicago Legal Forum*, 415. Retrieved from http://chicagounbound.uchicago.edu/uclfAvailableat:http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/11

Kim, E., & Julian, W. (2007). The ring of Gyges and legal ethics. *Legal Ethics*, *10*(1). doi:10.1080/1460728X.2007.11423879

Koops, T., Dekker, A., & Briken, P. (2018). Online sexual activity involving webcams—An overview of existing literature and implications for sexual boundary violations of children and adolescents. *Behavioral Sciences & the Law*, *36*(2), 182–197. doi:10.1002/bsl.2333

Lastowka, F. G., & Hunter, D. (2017). The laws of the virtual worlds. In *Popular Culture and Law* (pp. 363–435). London, UK: Routledge.

Lucatch, D. (2021, December). *Digital identity in the metaverse*. *Forbes*, Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/28/digital-identity-in-the-metaverse/?sh=661b74a1fb6b

McDougall, D. (2022, June). The metaverse has a sexual harassment problem and it's going to get worse. *Morning Brew*. Retrieved from https://www.morningbrew.com/daily/stories/2022/06/14/metaverse-has-a-harassment-problem

Microsoft Team. (2022). *Work trend index: Annual report, Great expectations: Making hybrid work work*.

Murphy, H. (2021). How will Facebook keep its metaverse safe for users. *Financial Times*, *12*. Retrieved from https://www.ft.com/content/d72145b7-5e44-446a-819c-51d67c5471cf?utm_source=dlvr.it&utm_medium=twitter

Naseh, M. V. (2016). Person and personality in cyber space: A legal analysis of virtual identity. *Masaryk University Journal of Law and Technology*, *10*(1), 1–21. doi:10.5817/MUJLT2016-1-1

Noval, S. M. R. (2021). *Cyberbullying Hak-Hak digital: Right on online safety*. Bandung, Indonesia: PT Refika Aditama.

Noval, S. M. R., Soecipto, & Jamaludin, A. (2022). *Perlindungan Hak Digital: Ancaman Privasi Di Tengah Serangan Social Engineering*. Depok, Indonesia: Rajawali Press.

Opsahl, K., & Rodriguez, K. (2021, June 2). *Your avatar is you, however you see yourself, and you should control your experience and your data* [Web log post]. Retrieved from https://www.eff.org/deeplinks/2021/06/your-avatar-you-however-you-see-yourself-and-you-should-control-your-experience-0

Parks, P., Cruz, R., & Ahn, S. J. G. (2014). Don't hurt my Avatar: the use and potential of digital self-representation in risk communication. *International Journal of Robots, Education and Art*, *4*(2), 10.

Seguin, B. (2010). Defamation of second life avatars: How the laws of first life people could be invoked. *Law School Student Scholarship*, 77. Retrieved from https://scholarship.shu.edu/student_scholarship/77

Siejca, R. (2023, February 13). *Exploring metaverse identity: Defining who we are online* [Web log post]. Retrieved from https://mazerspace.com/exploring-metaverse-identity-defining-who-we-are-online/

Spooner, M. A. (2012). It's Not a Game Anymore, Or is It: Virtual Worlds, Virtual Lives, and the Modern (Mis) Statement of the Virtual Law Imperative. *The University of St. Thomas Law Journal*, *10*, 533. Retrieved from https://ir.stthomas.edu/ustlj/vol10/iss2/7+

Union Avatars. (2023). *UnionID: Your digital identity for the open metaverse*. Retrieved from Union Avatars website: https://unionavatars.com/union-id/

Vogels, E. A. (2021). *The state of online harassment*. Retrieved from Pewresearch website: https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

Vorderman, C., Allen, C., & McIntosh, V. (2022). *Safeguarding the metaverse: A guide to existing and future harms in virtual reality (VR) and the metaverse to support UK immersive technology policymaking*. Retrieved from The Institution of Engineering and Technology website: https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf

Wolfendale, J. (2007). My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology*, *9*, 111–119.

Wong, Q. (2021, December). As Facebook plans the metaverse, it struggles to combat harassment in VR. *CNET*. Retrieved from https://www.cnet.com/tech/gaming/features/as-facebook-plans-the-metaverse-it-struggles-to-combat-harassment-in-vr/

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.