

Are virtual persons (avatars) subject to human rights protection? Should they be?

Gergely G. Karácsony

Metaverse – especially when paired with virtual reality headsets – provide users with a truly immersive experience. These virtual spaces are used for many purposes: work, school, gameplay and for socialising with others. The metaverse, however, comes with its own risks: harassment, bullying, and other violation of a person's rights are often reported. In this article, we examine whether fundamental rights protection could extend to virtual spaces as well, especially when the subject of such violations is not a human person directly, merely the avatar which represents them in the virtual world.

I. RULES INSIDE THE METAVERSE

Perhaps the biggest technological sensation of the past few years has been the development of open virtual spaces, popularly known as the metaverse. The expectations were high for this technology, which is clearly demonstrated by the fact that one of the world's biggest online service providers, Facebook's parent company, has changed its name to Meta. These interfaces can be used on a personal computer or mobile device, and to the fullest extent with virtual reality (VR) devices. Their possibilities of use are almost endless: starting from recreation and the creation of imaginary virtual worlds for entertainment purposes, through educational and workplace collaboration tasks, to virtual gatherings with family members and friends who live far away, they have proven to be a good solution in many areas of life. In virtual spaces, the user creates his own digital alter ego first: this avatar will personify him towards other users of the metaverse. The avatar is moved by the user; if VR devices are used, the digital alter ego maps the user's hand movements, its body and head turns together with the user. In the metaverse, users can communicate with each other verbally (with the help of a microphone) or in writing; the participants of the virtual space usually only know the user name (nickname) of the other person. The virtual worlds created in this way can be freely navigated, it is not pre-determined where users should go or what tasks they should perform. An example of these free virtual worlds is Horizon, a space developed by Meta that can be used with VR devices. The spaces of some online multiplayer games, such as Fortnite or Roblox, also function as a quasi-metaverse. In this study, we examine whether digital persons created in virtual spaces, avatars, are entitled to certain fundamental rights and whether they receive legal protection in the same way as "real" people. Our starting assumption is that where people (or the characters they control) are present in numbers, it soon becomes necessary to lay down a system of rules to ensure peaceful coexistence. We assume that certain fundamental rights related to individuals, such as the protection of personal data

and personality, as well as the prohibition of discrimination, require enforcement in the metaverse as well.

With these digital technologies on a rapid rise, we can observe the tendency of the decentralisation of their regulation, where the rule-making role of governments wane, giving way to interest groups and other participants within the industry,¹ who try to prevent the negative effects by developing industry standards and good practices. This kind of decentralization of regulation can be explained on the one hand by the rapid speed of technical development, and on the other hand by the devaluation of the regulatory role of traditional legislators.² This can also be observed in relation to the increasingly widespread virtual spaces. Entering the metaverse, an entirely new world opens before our eyes, in which we can act freely. However, this virtual world also has its rules: what “physical” laws does our avatar obey (for example, how it moves in space), how it interacts with its environment (can it transform the layout of the virtual space, can it create new elements in the space), and with other users (can they see each other, talk, or otherwise contact each other). These rules are determined by the software framework of the given virtual world, the developer pre-coded the operating rules into the program. However, more important to us are the “norms of conduct” in the metaverse world. They determine what a user should and shouldn’t do: in other words, what behaviour is allowed and what is prohibited.

Some rules have a clear legal background. The legislative and law-enforcing bodies focus primarily on communication: if the exchange of messages between the players clearly constitutes a crime, or is aimed at preparing or inciting a criminal act, the competent authorities will quickly intervene. An important example of this would be the sharing of content related to child pornography. Several precedents show that law enforcement agencies - in cooperation with the developer of the virtual environment - can collect evidence on the suspect, seize data contained in the virtual account, and even obtain data about the real-world identity the real person behind the player created in the virtual space. Similarly, authorities can monitor communication in the virtual space if they suspect that a terrorist act or other serious crime is being prepared there. However, the common feature of these cases is that the virtual space is used merely as a tool, a communication or data sharing channel for other crimes taking place in the real world (making of illegal pornographic recordings, acts of terrorism, etc.). In these cases, the intervention of the regulatory body or the law enforcement agency is justified by the fact that the illegal act taking place in the virtual space also has an impact in the real world; the real persons who actually carry out the criminal act in the outside world are the ones who merely re-directed part of their activities to the virtual world.

The subject of our investigation now are those cases where a behaviour is realized exclusively in the virtual world, among the actors present within, and does not constitute an explicit criminal act in the real world. An example for this could be harassment or stalk-

¹ Guihot / Matthew / Suzor.

² Villaronga / Golia, 132.

ing carried out in the virtual space, by constantly following one avatar against their will, intruding their “private space” within the virtual world. The behaviour shown in the virtual world - if it does not constitute an explicit crime in the manner described in the previous paragraph - is not or is only scarcely regulated by law. As soon as it comes to the in-game interaction of two users, we are already transferred to the territory regulated by the contractual terms and conditions of the company providing the virtual space, alongside the “community guidelines” they created (for example, the Code of Conduct for Virtual Experiences for the Horizon virtual world created by Meta).³ In most cases, the law does not cover interactions between characters that exist only in the virtual world, except when they have an impact on the outside world and on the natural person users behind the avatars. The community guidelines prohibit certain behaviours, among the rules of conduct of the virtual world of Meta, for example, we find the following:

Don't do or promote anything that is designed to deceive other users, Meta, developers, or that otherwise abuse our products or services, such as:

- Pretending to be another person or entity, stealing someone's identity, or creating or using fake accounts

- Engaging in fraud, scams, or other deceptive activities

- Gathering or sharing sensitive personal information, engaging in unauthorized access, or sharing malware.

Don't do or promote anything that's illegal, abusive, or could lead to physical harm, such as:

- Sexualizing, exploiting, or abusing minors

- Bullying, harassing, stalking, or hateful behavior

- Advocating, engaging in or promoting violence, human exploitation, human trafficking, or human smuggling. Supporting or representing groups or individuals involved in terrorism, hate-based organizations, or criminal groups

- Promoting or coordinating acts of physical harm, such as sexual or physical assault, or suicide or self-harm

- Any form of non-consensual intimate activity,

- Violating intellectual property rights, such as improperly using copyrighted or trademarked materials

- Unlawfully selling, exchanging, or promoting, regulated goods

Violators of the prohibitions are subject to sanctions within the system: a fixed-term or permanent ban, preceded by a warning or the temporary suspension of the account. The developer provides a complaint interface for “victims” of behavior that violates community guidelines, as well as built-in defense mechanisms in some cases (Meta, for example, allows you to set up a “personal space” around the character in the virtual world, where

³ Code of Conduct for Virtual Experiences. <https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/code-of-conduct-for-virtual-experiences/>.

no other user can enter). However, they introduce these at their own discretion, in order to create a better gaming experience and reduce the number of user complaints; they are also entitled to unilaterally modify them at any time. In this study, we argue that it would be necessary to define minimum standards protecting the “fundamental rights” of avatars existing in virtual space; these standards should be mandatory everywhere, regardless of the actual platform, and the enforcement must be ensured by the developers of all virtual environments. These minimum standards could be found among the human rights requirements laid down in international conventions, such as the European Convention of Human Rights and the International Covenant on Civil and Political Rights adopted by the United Nations. In this study, we examine the applicability of certain cases of the right to the protection of privacy (and of personal data), as well as the prohibition of discrimination.

II. WHY IS IT NECESSARY TO PROTECT THE FUNDAMENTAL RIGHTS OF CHARACTERS THAT EXIST ONLY IN VIRTUAL SPACE?

This is the first question that arises in connection with the topic, since at first glance it seems just as far-fetched and (for now) an academic issue as granting legal personhood to AI robots.⁴

The fundamental rights protection of the inhabitants of virtual spaces is not intended to protect the digital characters themselves from violations. According to the logic of fundamental rights, the subject of fundamental rights can only be a natural person, that is, a human being. It is no different in relation to the basic rights of the metaverse: they ultimately protect the person behind the avatars by protecting the digital person they control. In order for the proposed fundamental rights protection to be applicable, it is necessary to define the cases where the impact suffered by the virtual character can spread to the person behind it. Our current understanding of law cannot handle the situation when two digital characters cause each other privacy violations in the virtual space.

For the purposes of this article, we exclude such virtual spaces and behaviors where the user enters the virtual environment in the first place with the awareness and with the aim that the character he controls may suffer a disadvantage: for example in shooting games or combat based role-playing games. In this case, the known and accepted part of the game is the hostility between the characters, the in-game fight with an uncertain outcome. However, we can imagine several other cases where the character may be violated in the virtual space, and this also affects the user behind the character – without having real world impact assessable by law enforcement.

1. The situation is clear when the user has a specific business interest attached to the digital character. The complex monetization systems behind video games and other virtual activities can provide users with significant income.⁵ In many cases, a well-known

⁴ See: Papakonstantinou / De Hert and Keserű.

⁵ Király.

player, streamer or performance artist uses a character developed in detail and built up over a long period of time. The virtual personality personified in this way is part of the business model, so the infringement on it can actually be examined as damage to the user's business. In the future, however, we will not talk about business grievances.

2. The second case to be considered is when the harm (especially concerning privacy and data protection), suffered by the virtual person directly reflects back on the human user behind it. Such is the case when a conclusion can be made concerning the personal data and personality traits of the actual user, from the behavior shown by the character in the virtual world. Below we show why this is important even if the user in the metaverse does not behave in a way that corresponds to their everyday personality.

3. The third category of cases is the furthest away from direct harm to the person. In this case, we can speak of a specifically psychological effect, which affects the human user as a result of the harm suffered by the virtual character. As virtual characters are more and more often equipped with human-like features, an own individuality and realistic appearance, it becomes easier for us humans to form an attachment towards them. Thus, the injury to these characters, or their complete destruction, means a real mental shock for the person attached to them, just like the loss of a beloved pet. The possibility of bonding with human-like robots has already been demonstrated by several empirical studies in recent years.⁶ In the last decade, several researches have specifically examined our relationship with virtual characters, i.e. characters without a physical dimension. The virtual expression of emotions affects the degree to which recipients perceive a virtual character as human-like. In their research, Coanda and Aupers (2021) examined the built-in characters in computer games that are not operated by the players (these are called NPCs, non-player characters). The research established that fictitious virtual characters are humanized by the players, i.e. they are endowed with characteristics, motivations, and emotional states that are intrinsically human. Identification with the characters is enhanced if the given character can display realistic emotions as authentically as possible. Since people tend to reflect the emotional state of another person, it is conceivable that the emotional state of virtual characters that are human-like and capable of displaying realistic emotions can also be "transmitted" to the recipient, that is, to the human person observing or controlling them.⁷ If the receiver sees a virtual character suffering and enduring pain, then they may experience emotional distress as a result.

In this case, the "humane" treatment of virtual characters may not be prescribed by the legislator for the protection of the avatar itself, but because cruelty to them - due to the reflection of emotions and the bond formed with the character - may affect the observing person as the recipient as well. As a moral argument, we can put forward the position that also appears in academic literature, according to which the cruel treatment of robots - just like animal torture or animal experiments - casts a bad light on humanity as a whole and should therefore be banned.⁸

⁶ Broadbent, 634-635.

⁷ Horváth, 137.

⁸ Ashrafian, 32-34.

Based on the above, we can conclude that the legal protection of characters and avatars existing in virtual space may be justified in certain cases. They don't deserve legal protection in themselves, but for the protection of the humans behind them, who observe or control them. One of the characteristic features of virtual spaces is anonymity, that is, the fact that it is not possible for the other participants to know who is/are behind each virtual character. It is even less clear who and how many people watch the events passively, through various media channels or through opportunities provided by the virtual space itself. Legal protection in the traditional sense, as well as the legal standing under fundamental rights protection, usually assume that a specific, natural person is identifiable as their subject. The person entitled to legal protection, i.e. the person who can act against the violation, must necessarily be a natural person (or possibly a legal person). In the case of illegal behavior committed between or against digital characters in the virtual space, this very person, the natural person suffering the harm, is missing from the equation. In my opinion, the legal protection of virtual personalities is necessary precisely in those cases when we cannot identify who the natural person behind the avatar is.

In the following, focusing on some areas of fundamental law, we examine whether legal (and especially fundamental rights) protection can be applied in the case of digital personalities.

III. DOES AN AVATAR HAVE PERSONAL DATA?

The data protection regulation in force in the European Union is clear in that only the data that can be linked to natural persons can be considered personal data. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation - GDPR) defines personal data as any information relating to an identified or identifiable natural person ("data subject").⁹ Responding to the challenges of the information society, the European legislator interprets the concept of identifiability as broadly as possible: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. Moreover, identifiability is not an absolute category, but rather context-dependent. It is possible that in a certain environment the person concerned is not considered identifiable, but becomes identifiable in a different group of people or in a different situation. Thus, a situation can also be imagined in connection with the data concerning the actors of the virtual space, when they can be connected to the user behind it, while in other cases this information can be treated merely as metadata or as non-personal data. The mere fact that we do not connect to the virtual space by entering our full name does not eliminate the personal nature of the data collected during the activities carried out there. The fact that the service provider operating the virtual space receives information about the IP address of the computing device we use can establish the treatment as personal data. In recent years, the question has

⁹ Article 4 (1) of the GDPR.

arisen several times whether IP addresses used to identify computing devices connected to the Internet are considered personal data, especially given that dynamic IP addresses are redistributed by the Internet service provider to subscribers at specific intervals, and in some cases an IP address may include several IT devices. In 2016, the Court of Justice of the European Union also stated in its judgment¹⁰ that under certain circumstances, the dynamic IP address is also considered personal data. This is also supported by Recital 30 of the GDPR, according to which “natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”

We cannot go beyond the fact that the boundary between personal data and non-personal data is constantly changing, as is often pointed out in the literature.¹¹ Information currently treated as non-personal data may become personal data in the future (as a result of technological development), since new and new methods of use and analysis are constantly appearing, and more and more databases can be connected at the same time.¹² It should be also pointed out that anonymised data can also become de-anonymised by the use of modern technologies. In light of this, we have to examine the decision rights exercised over the data generated in virtual spaces and the metaverse and the question of the potential ownership of the data.

Research supports the fact that the registered self in virtual space (this includes online interfaces) is constructed specifically with the audience in mind.¹³ This self is usually characterized by expressivity, and often sharing intimate personal information and innermost thoughts.¹⁴ The personal data shared in this way is therefore information about the natural person behind the avatar. The data that can be learned about the natural person user through the virtual character, as well as the conclusions that can be drawn from them, are certainly entitled to protection. It may happen, for example, that a user only experiences his secret desires and impulses in the virtual space, which may cause dismay in society, are contradictory or even forbidden. In such cases, their behavior in the virtual space refers back to suppressed or hidden features of their personality, which according to the GDPR, may even fall in the special category of personal data (for example, in the case of health, addictions, sexual preferences or orientations). If we look at the virtual space as a kind of “protected playground”, then the user may have a legitimate expectation that the service provider will keep his in-game behavior a secret, not draw conclusions about the real person, and not use them for commercial (e.g. targeted advertising) purposes. A situation can easily arise where, in the apparently protected space

¹⁰ Case no. C582/14.

¹¹ Janeček, 1040.

¹² Wendehorst, 332.

¹³ Wang, 5.

¹⁴ Hollenbaugh; Stefanone / Jang; Lee / Im / Taylor.

of the game, the user also shows something of himself that he wants to keep secret from his environment or society (and here we are not referring to illegal activities). Therefore, receiving advertisements, product and service offers related to their behavior or preferences the next day may cause serious infringement of rights. It can be particularly worrisome if the service provider operating the virtual space forwards this information to third parties, and thus the user's behavior in the virtual space becomes part of the commercial personality profile created about him. It is also worth mentioning that the user may not behave in accordance with his real personality in the virtual space, but may try out a desired character or behavior "without stake" in order to observe the reactions of his in-game environment. It is also possible for the user to play a fictional character and display behavior appropriate to the role. In such cases, the conclusion drawn from the behavior or established personality trait will not necessarily be accurate and correct. This may also violate the principle of accuracy contained in the GDPR.¹⁵ Incorrectly drawn conclusions and the corresponding treatment of the user may harm the person's social reputation in the future, and may even (in certain religious or political regimes) expose him to real danger, retaliation or persecution.

We therefore believe that the correct behavior in terms of handling personal data is to separate the virtual space (the metaverse) from the real world. The information recorded in one place and the established conclusions cannot leak into the other space, as this may violate the privacy of the user and the basic principle of the GDPR regarding data accuracy. Of course, this view is difficult to implement in reality, since the basic interest of service providers is to collect as much data as possible about users and use them for commercial purposes.¹⁶ However, if this separation is successful, the user will have two personal spaces: virtual and real, in both of which he can show different characteristics. An example for this separation would be if the data collected in the virtual space could only be used to communicate with the user and send commercial promotions to him within the same virtual environment, and not outside of it (perhaps not even in the common "waiting area" of a game or similar virtual environment).

Overall, it can therefore be concluded that, according to the current regulations, an avatar created in the virtual space does not in itself have the right to the protection of personal data, since it is not considered a natural person. However, the real person behind the virtual character has the right not to have the "personal data" collected about the character directly or indirectly connected to him. However, this can be achieved in its entirety if we also create and enforce the digital avatar's right to data protection, otherwise the collected data exists in a "vacuum" and only acquires the character of personal data if – possibly as a result of a later technical development step – they become connectable to the specific user.

¹⁵ [Personal data] shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. (GDPR Article 5 point (1) b)).

¹⁶ Yu – Zhao.

IV. OTHER ASPECTS OF PRIVACY PROTECTION

The protection of privacy in the broader sense also includes the protection of private residences and private communications (privacy of correspondence). For a very long time, the public opinion was that, due to the secret channel that messages are exchanged in within video games in virtual spaces and game consoles, the communication of players remains hidden not only from the public, but also from the authorities. The series of attacks in Paris that claimed the lives of more than a hundred people in 2015 were also allegedly (although not proven) planned using the PlayStation network.¹⁷ The year 2018 brought upon a new situation in this issue, when Sony first shared communication data within the PlayStation Network with law enforcement agencies. With a proper court order, the FBI requested access to the messages of Isse Aweis Mohamud, a person who allegedly travelled abroad in order to join a terrorist organization.¹⁸ Although by several months delay, Sony complied with the request and handed over to the investigative authority the data related to the DejanWoW username, including information about the use of the game console, purchases within the system, and the messages exchanged by the user via the PS3 and PS4 systems.¹⁹ The case is novel in that this time the authorities did not subject the game console itself to investigation (as Mohamud carefully erased its contents), but the FBI requested and received access to the information stored in connection with the user account from the service provider operating the game system. From this case, it becomes clear to us that the user's messages are still in the possession of the service provider operating the system even after the complete deletion or destruction of the hardware, they can be retrieved later and their content can be recovered. Without exception, the data management policies of the examined service providers stipulated the retention of data in order to enforce legal claims and fight against illegal content. In addition to the fight against illegal content, the service providers also use the content of messages between users for other, technical purposes, which they inform the users about: the presumed purpose of data management is, on the one hand, the fight against fraud and violations of the terms of use, and thereby the protection of the interests of the company, in addition to these the data can also serve business and service development purposes. On the other hand, the purpose of data management may also be to provide the authorities with information proving the facts in case of specific violations. Finally, the management and preservation of chat data may be necessary in order to provide certain services.²⁰

¹⁷ see: Tassi.

¹⁸ Documents of the case 17-SW-00121-SWH. <https://www.documentcloud.org/documents/4378583-Sony-Data-Request-From-Law-Enforcement-Terrorist.html>.

¹⁹ <https://www.documentcloud.org/documents/4378582-Sony-PlayStation-PS4-Data-Handed-Over-in-Terror.html>.

²⁰ see in detail: G. Karácsony.

V. CAN THE AVATAR BE SUBJECT OF DISCRIMINATION BASED ON ONE OF ITS CHARACTERISTICS?

Finally, it is worth discussing some of the core forms of discrimination, as possible forms of violations of rights against actors existing in the virtual space. In order to determine whether this poses a realistic threat to actors in the metaverse, we must perform the first two steps of the discrimination test: examining whether a disadvantage occurred, and judging whether it was based on the protected characteristic.

Discrimination is particularly interesting in connection with the virtual space, since in this case it is almost certain that the basis of the discrimination is not some characteristic, feature or condition of the real person behind the affected avatar. The properties that can be considered are usually carried by the avatar itself, but they are not at all certain to be matched to the properties of the user behind it. It often happens that men choose a female virtual character for themselves, or vice versa. In the same way, the skin color, body shape, hairstyle and other characteristics of the avatar can be customized (in some virtual worlds, you can also play with creatures belonging to different species). However, these characteristics can differ from the characteristics of the user controlling the character, but they can also be the same: you can create an exact virtual copy of yourself. However, the important feature of these situations is that other users interacting with the avatar only see the avatar's external features, not that of the person behind it. Thus, if they are treated adversely, it can only be based on the characteristics of the virtual character, which in some cases may match the characteristics of the actual user, but the other party cannot be sure of this. So the protected characteristics exist, just like in the real world, but in our case they are not carried by the user, but by the avatar. Thus, discrimination on the basis of the characteristics of the human person may not take place, however, discrimination by association, a term that was developed through international legal literature and jurisprudence, may be established. This concept covers cases where a person suffers disadvantageous treatment because of certain characteristics of another person who is related to them. Such a case is, for example, when a mother raising a child with a chronic illness is at a disadvantage when looking for a job. In this case, the child's illness is the basis of discrimination, but the disadvantage does not affect the child, but the parent. Discrimination due to certain characteristics of the virtual character can therefore occur in the same way for the person controlling the character, despite the fact that he does not (necessarily) carry the protected characteristic.

Unfavorable treatment and discrimination can take many forms in the virtual space. On the one hand, it is possible that due to its protected nature, the digital actor is not allowed to enter certain places, or is excluded from some activity in which the user wants to participate. There is not a large amount of documented cases or user reports on this issue yet. However, the literature also raises related theoretical cases. It is very likely that in virtual worlds, users with the same interests or similar characteristics form close-knit virtual societies, so-called cloud communities.²¹ Users belonging to various social minor-

²¹ Orgad, 257.

ities (for example, people with LGBTQ+ identity) will certainly be happy to create such virtual communities, where they can freely live according to their identity, which in the real world might be subject to contempt or even persecution. The fact that the service provider operating the virtual platform allows the formation and operation of such communities, lets users join them, or even regulates them at all, raises the question of discrimination and the equal enjoyment of rights and freedoms. Belonging to such cloud communities can in itself be the basis for discrimination in other parts of the virtual space - if the service provider or other users are aware of this fact. Belonging to a cloud community based on protected properties is in itself sensitive information that the platform provider can only handle with the utmost care and under special safeguards. The service provider regulating the virtual space therefore actually decides on human rights and fundamental freedoms in these cases.²²

During the period when this study was published, a case caused a lot of upheaval, which involved behavior that can traditionally be classified as discrimination: a user reported that his avatar had been the victim of sexual harassment or rape.²³ According to her, another user followed her and regularly entered the character's personal space after, with the encouragement of others, the aggrieved party turned off the security zone around his character, which was in place to prevent such incidents. After that, in front of other users, he engaged in a sexual act with her virtual avatar, without her consent. The touches and caresses were transmitted to her in the form of vibrations by the victim's VR device. In this case, the basis of the harassment was the female gender of the virtual character, as a protected characteristic. This example highlights that harassment of virtual characters is a real phenomenon, and the user controlling the character experienced it as an attack as intense as if it happened to her in real life.

VI. CONCLUSIONS

In summary, it can be said that the digital characters of the metaverse are in some ways just as vulnerable to negative effects on their personal rights as the users who control them in real life. Legal disadvantages affecting avatars sometimes pose a threat to the human users behind them, sometimes directly (for example, through the personality profile that can be built), and sometimes indirectly, through their psychological effect. For the time being, the fair treatment of avatars in virtual worlds is not prescribed by a mandatory rule, and is only supported in a few places by the terms of use and community guidelines of the given interface. We find that fundamental rights protection - as it is laid down in major international conventions - could also provide adequate guidelines regarding the behavioral norms of the metaverse. Current legislation painfully lags behind technical developments, for example the law, which predominantly considers physical interaction as a prerequisite for sexual assault, might be inadequate for dealing with crimes in

²² Charamba, 124.

²³ It happened in Meta's virtual space, Horizon's World. <https://www.independent.co.uk/tech/rape-metaverse-woman-oculus-facebook-b2090491.html>.

virtual environments. Currently, users that experience abuse in the virtual space, have nowhere to turn, and therefore may feel abandoned and helpless. It is also unclear what the definition of abuse against occupants of the virtual space is, where the boundary between acceptable and unacceptable behaviour lies. The need for laws that recognize and criminalize non-physical but psychologically damaging forms of abuse in virtual spaces is therefore urgent.

The regulation of the metaverse also brings about ethical dilemmas. What happens when real world social norms and in-game rules conflict? Is there a reasonable expectation that a real-world social norm will be respected in the game? This question was raised by the infamous “Funeral Raid”, which took place more than a decade ago, in the virtual world of the game called World of Warcraft.²⁴ Here, the members of one of the in-game clans said goodbye to a fellow player, who died of a heart attack, with a “funeral” held in virtual space. The commemorators were attacked by their in-game enemy clan and most of them were killed. In the real world, it is absolutely clear that the privacy and dignity of funerals and those who participate in them are respected. This behavior would clearly mean the case of the violation of multiple personal rights in real life. However, World of Warcraft is specifically a fighting game, the essence of which is precisely that the members of opposing clans defeat each other. Thus, the attackers did not violate the rules of the game, in fact, they specifically acted in its spirit. However, when projected onto the real world, their actions caused outrage and pain to the commemorators, who mourned their friend, whom they lost in the real world, in the virtual space that provided a framework for their relationship.

BIBLIOGRAPHY

1. Printed volumes and journal articles

Hutan Ashrafian, *AlonAI: A Humanitarian Law of Artificial Intelligence and Robotics*, Science & Engineering Ethics 21(2015), 29–40.

Elizabeth Broadbent, *Interactions With Robots: The Truths We Reveal About Ourselves*, Annual Review of Psychology, 68 (2017), 634-635.

Kuzi Charamba, *Beyond the corporate responsibility to respect human rights in the dawn of metaverse*, University of Miami International and Comparative Law Review, 30(1) (2022) 110-149.

Iulia Coanda / Stef Aupers, *Post-human encounters: Humanising the technological Other in videogames*, New Media & Society, 23, 5 (2021).

²⁴ <https://www.gamesradar.com/the-wow-funeral-raid-four-years-later/>

Gergely G. Karácsony, A videójátékok adatkezelési gyakorlata: kommunikáció és profilalkotás, G. Karácsony Gergely (ed.), A videójátékok jogi kérdései, Széchenyi István Egyetem (2021).

Michael Guihot / Anne F. Matthew / Nicolas P. Suzor, Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence, 20 Vanderbilt Journal of Entertainment and Technology Law 385 (2020)

EE Hollenbaugh, Motives for maintaining personal journal blogs, Cyberpsychology, Behavior, and Social Networking 14(1/2) (2011), 13–20.

Evelin Horváth, Pixelekbe öntött érzelmek – A virtuális érzelm megjelenítés vizsgálatának lehetőségei, Századvég, 1. (2022)

Václav Janeček, Ownership of personal data in the Internet of Things, Computer law & security review 34 (2018), 1039–1052.

Barna Arnold Keserű, A mesterséges intelligencia magánjogi mibenlétéről, Lévaýné, Fazekas Judit / Kecskés, Gábor (eds.), Az autonóm járművek és intelligens rendszerek jogi vonatkozásai, Universitas-Győr Nonprofit Kft (2020).

Péter Bálint Király, A videójátékok monetizációjának jogi kérdései. G. Karácsony Gergely (ed.), A videójátékok jogi kérdései, Széchenyi István Egyetem (2021).

D-H Lee / S Im / CR Taylor, Voluntary self-disclosure of information on the internet: A multimethod study of the motivations and consequences of disclosing information on blogs, Psychology & Marketing 25(7) (2008), 692–710.

Liav Orgad, Cloud Communities: The Dawn of Global Citizenship?, Debating Transformations of National Citizenship, Rainer Bauböck ed. (2018).

Vagelis Papakonstantinou / Paul De Hert, Structuring modern life running on software. Recognizing (some) computer programs as new “digital persons”, Computer Law & Security Review 34 (2018) 732–738.

MA Stefanone / C-Y Jang, Writing for friends and family: The interpersonal nature of Blogs, Journal of Computer-Mediated Communication, 13(1) (2008), 123–140.

Eduard Fosch Villaronga / Angelo Golia Jr, Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance, Computer Law & Security Review 35 (2019) 129–144.

Qi Wang, The triangular self in the social media era, Memory, Mind & Media, 1 e4 (2022), 1–12.

Christiane Wendehorst, Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy, Lohsse, Schulze and Staudenmayer (eds): Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III (2017), 327 - 356.

Xiaolan Yu / Yun Zhao, Dualism in data protection: Balancing the right to personal data and the data property right, *Computer Law & Security Review* 35 (2019).

2. Online resources

Code of Conduct for Virtual Experiences. <https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/code-of-conduct-for-virtual-experiences/>

Woman says she was virtually ‘raped’ in the metaverse while others ‘passed around a bottle of vodka’ (The Independent online, 2022.) <https://www.independent.co.uk/tech/rape-metaverse-woman-oculus-facebook-b2090491.html>

Documents of the case 17-SW-00121-SWH.

<https://www.documentcloud.org/documents/4378583-Sony-Data-Request-From-Law-Enforcement-Terrorist.html> (2023.09.07.)

<https://www.documentcloud.org/documents/4378582-Sony-PlayStation-PS4-Data-Handed-Over-in-Terror.html> (2023.09.07.)

The WoW funeral raid – four years later. Gamesradar, 2010. <https://www.gamesradar.com/the-wow-funeral-raid-four-years-later/>

Paul Tassi, How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks, *Forbes Online*, 2015.11.14. <https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/?sh=3337aa247055>