Empowering personal data sovereignty in hyper-realistic Metaverse avatars through blockchain technology

Natalia Menéndez González*

Abstract: Avatars are digital representations of oneself used within virtual environments to portray ourselves in the form of our choice. Avatars have taken many shapes and styles since their first appearance in the digital domain. Because of this, new digital environments, such as Metaverse ones, will require a reinvention of this concept, one where it will gain more importance. The better the avatar, the more immersive and realistic the Metaverse experience. In this context, Meta is currently working on a new form of avatars, hyper-realistic ones, which perfectly mimic a full-body digital image of a person. While the possibilities this kind of avatar might entail for immersion and entertainment are undoubted, the risks the use of these avatars might entail from a privacy and data protection perspective are yet to be seen. Considering the quantity and nature of data collected and processed to create these avatars, they can be considered personal data and, in some cases, even biometric data. Thus, in the European Union, the processing of such personal and biometric data should comply with several restrictive conditions imposed by the General Data Protection Regulation. This paper will discuss the lack of clarity about the legal status of personal data from Metaverse avatars. Further, the contribution will propose using blockchain technology as a privacy-enhancing technology, which might help Metaverse users retain control of their personal data. In this regard, blockchain offers a promising alternative due to its decentralized, immutable and transparent nature maintaining privacy and confidentiality at the same time. Finally, the paper will examine the potential benefits of using blockchain technology to ensure avatar interoperability between virtual worlds in the Metaverse from a legal perspective.

Keywords: Metaverse, Hyper-realistic avatars, Data protection, Personal data, Biometric data, Blockchain

1. Introduction

From science fiction depictions of the Metaverse to real ones, the crucial role that avatars play within the Metaverse ecosystem is unquestioned.[1] Avatars are vital to enhancing users' interaction,[2] and, in this manner, users employ them to express themselves in many ways. Some choose 'fantastic' avatars to portray themselves as dinosaurs, zombies or robots. Others use their avatar to show how they identify themselves.[3] In other cases, some choose their avatar to deceive people for diverse purposes, including criminal ones such as grooming.[4]

Probably one of the most popular and intuitive options is using realistic avatars, meaning avatars that resemble, with better or worse accuracy, the user's physical appearance. In this regard, avatar design probably reached a milestone with Kodak's hyper-realistic Metaverse avatars, introduced during a podcast interview between Mark Zuckerberg and Lex Fridman in September 2023.[5] Such avatars entail a significant leap in terms of Metaverse interaction, making it even closer to face-to-face communication.

However, the more similar Metaverse avatars are to human representations, the more personal data they

* PhD candidate, Law Department, European University Institute and Research Associate, Centre for a Digital Society, European University Institute.

1 See, for instance, the symbolism of digital avatars within the novel by E. Cline, *Ready Player One* (Arrow Books, 2018) and its film adaptation in 'Ready Player One—Symbols—CliffsNotes', available at: https://www.cliffsnotes.com/literature/ready-player-one/symbols (accessed 6 May 2024).

2 Hyun-Woo Lee and others, 'How avatar identification affects enjoyment in the metaverse: the roles of avatar customization and social engagement' (2023) 26 Cyberpsychology, Behavior, and Social Networking 255, available at: https://www.liebertpub.com/doi/abs/10.1089/cyber.2022.0257 (accessed 6 May 2024).

3 Daniel Zimmermann, Anna Wehler and Kai Kaspar, 'Self-representation through avatars in digital environments' (2023) 42 Current Psychology 21775, available at: https://doi.org/10.1007/s12144-022-03232-6 (accessed 6 May 2024).

4 Sameer Hinduja, 'Child grooming and the metaverse – issues and solutions' (*Cyberbullying Research Center*, 9 April 2024), available at: https://cyberbullying.org/child-grooming-metaverse (accessed 6 May 2024).

5 *Mark Zuckerberg: First Interview in the Metaverse | Lex Fridman Podcast #398* (directed by Lex Fridman, 2023), available at: https://www.youtube.com/watch?v=MVYrJJNdrEg (accessed 20 February 2024).

10.4337/ielr.2025.01.04

Figure 1 The avatar of Mark Zuckerberg (left) is a digital depiction rendered in real-time (centre) via the use of a Quest Pro headset (right)

Source: https://conecta.tec.mx/en/news/national/society/hyperreal-avatars-turning-point-virtual-interaction

reveal about the Metaverse user. In this regard, if we look at Figure 1, it is relatively easy to grasp a very accurate representation of Mr Zuckerberg's facial image, even if we have not seen any picture of him before. Further, since hyper-realistic Metaverse avatars represent the full body of a person, it is also possible to make an impression of their height (particularly compared to other avatars), their movements or their body shape, to name some characteristics. Some of these characteristics have been considered personal data, special categories of data and/or biometric data by the European Union data protection legislation. Therefore, the existence of hyper-realistic Metaverse avatars poses an interesting question from both a privacy and data protection perspective, being their legal status.

This paper will discuss the legal regime applicable to hyper-realistic Metaverse avatars from a European Union privacy and data protection perspective. Being the European Union a role model[6] in terms of fundamental rights protection in general and privacy and data protection in particular, the legal status of hyper-realistic Metaverse avatars will be put to the hardest test. Further, once the legal status of hyper-realistic Metaverse avatars is established, the paper will study their data governance regime. Finally, the paper will propose the use of blockchain technology for Metaverse avatar data governance as a privacy-enhancing solution. Blockchain technology has been chosen in this respect due to its decentralized, immutable and transparent nature. The paper will close with the conclusions of the research.

Before delving into the legal status of Metaverse avatars, it is necessary to briefly examine what these avatars are, which role they play within the Metaverse environments and more specifically what (if anything) makes hyper-realistic Metaverse avatars particularly worth attention from a privacy and data protection perspective.

2. A hitchhiker's guide to Metaverse avatars

The term 'avatar' derives from Sanskrit and may be interpreted as incarnation or God's presence on Earth. In Hindu mythology, a God named Vishnu is said to have visited the world nine times to combat evil. For each visit, he assumed a different embodiment, known as an avatar.[7] The word avatar was initially used in the context of virtual worlds in the pioneering Habitat system

6 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2019), available at: https://academic.oup.com/book/36491 (accessed 5 March 2024).

7 'How gaming turned a hindu concept into the internet's most common feature' (*Inverse*, 20 February 2024), available at: https://www.inverse.com/gaming/avatar-meaning-origins-video-games (accessed 7 May 2024).

of the mid-1980s, and it was popularized by Stephenson's science-fiction novel Snow Crash in 1992.[8]

According to Meta, '[a]vatars are a digital expression of you, letting you freely express your identity, personality and appearance'.[9] From an academic perspective, however, there is no strong consensus on a unified definition of avatars.[10] In this line, Miao and others state that

'Academics have used multiple terms interchangeably to refer to avatars, such as automated shopping assistants (Al-Natour, Benbasat, and Cenfetelli 2011), chatbots (Ho, Hancock, and Miner 2018), virtual customer service agents (Verhagen et al. 2014), embodied conversational agents (Bickmore, Pfeifer, and Jack 2009; Lee and Choi 2017; Schuetzler et al. 2018), or virtual/digital assistants (Chattaraman et al. 2019; Freeman and Beaver 2018)'.[11]

For this paper, we will adopt the definition of Davis and others building on the work of Bailenson and others: '[a]n avatar is defined as a user-created digital representation that symbolizes the user's presence in a metaverse'.[12]

An avatar is an alter-ego of the Metaverse user. It communicates what the user wants the other Metaverse users to know about themselves.[13] On the one hand, the presence of Metaverse avatars enhances the Metaverse experience, since users need a digital representation to allow them to interact with the virtual worlds, their components and the other users. And the more accurate the avatar is to the physical representation of a person, the closer to a real-world experience the Metaverse interaction will be. On the other hand, the existence of Metaverse avatars can also entail a great deal of legal problems. First, as previously mentioned, the use of Metaverse avatars to commit both civil and criminal illicit such as threats, harassment, stalking, fraud, identity theft, defamation, grooming or online raping.[14] Second, the legal problems arising from the design, creation and existence of the avatars themselves and the personal data they might reveal. This second set of problems will be the object of this contribution.

In this regard, particular attention will be paid to hyper-realistic Metaverse avatars. Hyper-realistic Metaverse avatars represent, to the knowledge of the author, up to now, the most faithful representation of a person's physical appearance within an avatar's shape. According to Schiefelbein, '[h]yper-realistic avatars (HRAs) are video representations of a person with the mannerisms, vocal qualities, and production capabilities that come close to mirroring the same human performing a script for video'.[15] Further, they are 'custom-created digital embodiments of a real human, created by combining a captured video and vocal likeness'.[16]

As previously mentioned, Kodak's hyper-realistic Metaverse avatars became mainstream after their appearance during a podcast interview between Mark Zuckerberg and Lex Fridman in September 2023. According to Fridman,

> [t]his technology is incredible and I think it's the future of how human beings connect to each other in a deeply meaningful way on the internet. These avatars can capture many of the nuances of facial expressions that we humans use to communicate and motion to each other.[17]

According to Zuckerberg, the idea behind Kodak's hyper-realistic Metaverse avatars is that

> Instead of our avatars being cartoony and instead of actually transmitting a video, what it does is we've scanned ourselves and a lot of different expressions, and we've built a computer model of each of our faces and bodies and the different expressions that we make and collapsed that into a Kodak that then when you have the headset on your head, it sees your face, it sees your expression, and it can basically send an encoded version of what you're supposed to look like over the wire. So, in addition to being photorealistic, it's also actually much more bandwidth efficient than transmitting a full video or especially a 3D immersive video of a whole scene like this.[18]

Zuckerberg justifies the added value of Kodak's hyper-realistic Metaverse avatars stating that there have been several studies that show that the majority of communication, even when individuals talk, is not about the words

8 Michael Gerhard, David Moore and Dave Hobbs, 'Embodiment and copresence in collaborative interfaces' (2004) 61 International Journal of Human-Computer Studies 453, available at: https://www.sciencedirect.com/science/article/pii/S1071581904000126 (accessed 7 May 2024).

9 'Meta – Shop VR headsets & smart glasses' (*Meta*), available at: https://www.meta.com/ (accessed 6 May 2024).

10 Fred Miao and others, 'An emerging theory of avatar marketing' (2022) 86 Journal of Marketing 67, available at: https://doi.org/10.1177/0022242921996646 (accessed 6 May 2024). This publication contains a very comprehensive overview on 'Avatar Definitional Elements in Empirical Research' (Table 1).

11 Ibid 68.

12 Alanah Davis and others, 'Avatars, people, and virtual worlds: foundations for research in metaverses' (2009) 10 Journal of the Association for Information Systems 90, available at: https://aisel.aisnet.org/jais/vol10/iss2/1/ (accessed 7 May 2024).

13 Mary Anne Franks, 'Unwilling avatars: idealism and discrimination in cyberspace' (2011) 20 Columbia Journal of Gender & Law 224.

14 Ben Chester Cheong, 'Avatars in the metaverse: potential legal issues and remedies' (2022) 3 International Cybersecurity Law Review 467, available at: https://link.springer.com/10.1365/s43439-022-00056-9 (accessed 7 May 2024).

15 'Human vs machine: hyper-realistic avatars and their efficacy as a communication channel – ProQuest' 7, available at: https://www.proquest.com/openview/9888649da11617e0634e3563a44e85b1/1?pq-origsite=gscholar&cbl=18750&diss=y (accessed 7 May 2024).

16 Ibid 10.

17 See (fn 6).

18 Ibid.

they say. It is about the expressions they use. And Meta attempted to convey it with the traditional expressive avatar technology they used. Those were more cartoonishly created, but it was still possible to apply expressions to those faces as well. But there is certainly a level of realism that comes with presenting this photorealistic experience that, in Zuckerberg's words, goes to the heart of the aim of virtual and augmented reality: to provide a sensation of presence as if you were all there, no matter where you are in the world.[19]

The process starts with a small number of people doing these very detailed scans, and before that, Zuckerberg claimed that they would probably need to over-collect expressions when they were scanning because they had not figured out how much they could reduce that down to a streamlined process and extrapolate from previous scans. However, the objective – for which Meta already has a project underway – is to conduct a very brief scan using one's phone, in which you simply hold it in front of your face for a few minutes, speak a few sentences and make a variety of expressions. The entire process should take no more than two to three minutes, after which you will have your hyper-realistic avatar.

According to Zuckerberg, that is one of the big challenges that remains, and right now they can do the scans if one has hours to sit for one, but the production of these scans in a very efficient way is one of the last pieces that Meta still needs to overcome. And then, there are all the experiences around it. Part of the vision for this over time is not just having to be a video call, but one can do a video call on their phone.

The Metaverse allows one to accomplish things that you cannot do on a phone, such as participating in activities together. And, according to Zuckerberg, we could play games like these. We could have gatherings like this in the future. Once mixed reality and augmented reality are available, we may use Kodak Avatars to attend a conference and have some people there while others appear in this photorealistic form superimposed on the physical setting. In Zuckerberg's words, there is still a lot of tweaking that Meta would need to do where various people emote to varying degrees, so one of the key questions is, how broad is your smile? And how broad would you like your smile to be? And one of the things they would have to find out is how to fine-tune it on an individual basis. 'It's like, how much control do you want to give people over that? Some people may choose an expressive depiction of themselves in their avatar rather than their genuine faces'.[20]

There is also a debate about how one might want to adjust it, but ultimately, Meta wants to start by capturing how individuals feel and express themselves. And, according to Zuckerberg, they have moved past the uncanny valley. One of the challenges Meta experienced with some of their virtual reality and mixed reality work was that it seemed much deeper when one was in it than when they were watching 2D footage of the experience. According to Zuckerberg, that answers to the fact that the avatar is photorealistic, it will appear as great in 2D as it does to those who are in it.

The goal is to introduce Kodak's hyper-realistic Metaverse avatars gradually over time. To do so, Meta should scan and enrol more individuals in the system. After that, they want to start integrating it into all of their applications, which will improve productivity for many aspects of work–life balance. For remote meetings, something similar may, therefore, be beneficial. In addition, having the ability to hold remote meetings and other events where one is just having hangouts with friends will be especially helpful with the upcoming release of Meta Quest Three, which would be the first widely available mixed reality product in which one can take digital representations of people or objects and overlay them on the real world. As a result, Meta's ambition is to roll Kodak's hyper-realistic Metaverse avatars out over the next few years. They are not currently ready to be a popular product, but they will continue to improve it, add additional scans and expand its functionality.

Another aspect is that, after one gets the scan, processing it – both for the headset's sensors and for rendering – requires a certain amount of processing power. Therefore, one of the issues Meta is addressing is about the ideal fidelity level. The entire body could be done in a Kodak, which can be fairly involved, but one of the ideas they are considering is that, while it is possible to stitch a version of one's body with some major movements and a somewhat lower fidelity, their resolution for reading and expressing emotion is highest on one's face. For instance, shifting one's eyebrows by a millimetre significantly alters one's expression and conveys a different message than shifting one's arm by an inch, which is probably not as noticeable. Thus, according to Zuckerberg, the idea is to focus the computing power in the face and part of the work for the upcoming period will go towards that.[21]

Therefore, Kodak's hyper-realistic Metaverse avatars signify the next frontier in terms of avatar representation. However, in the same way that online presence and interaction might reveal a great deal of data, sometimes even

19 Ibid.
20 Ibid.
21 Ibid.

personal data, about a person, their virtual representation might do so as well. Thus, the next section will focus on the legal regime of Kodak's hyper-realistic Metaverse avatars under European Union law, particularly the General Data Protection Regulation (GDPR).[22]

3. Are hyper-realistic metaverse avatars personal data?

According to Article 4(1) GDPR,

> "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one 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 of that natural person.

As widely discussed by the scholarship[23] and the case law of the Court of Justice of the European Union (CJEU),[24] the 'identifiability' criterion is the key question to consider whether a certain piece of information (a Kodak's hyper-realistic Metaverse avatar in this case) constitutes personal data. According to Article 29 of Data Protection Working Party,[25] 'in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it […]'.[26] Further, '[i]dentification is normally achieved through particular pieces of information which we may call "identifiers" and which hold a particularly privileged and close relationship with the particular individual. Examples are outward signs of the appearance of this person, like height, hair colour, clothing, etc …'. In principle, considering the high level of detail of Kodak's hyper-realistic Metaverse avatars, it seems plausible that they allow the identification of a subject. They show some of the information mentioned previously (such as hair colour) but also so much more. Further, attending to the 'distinguishability' criteria, Kodak's hyper-realistic Metaverse avatars allow one to identify a person, for instance, Mark Zuckerberg vs. Lex Fridman within the interview they conducted.

Attending to the information provided by Mr Zuckerberg in the podcast interview, it is relatively safe to assume that photorealistic avatars will be pretty straightforward to allow the identification of a person. Even if the level of detail regarding the body was sacrificed in favour of the accuracy of the face, as he mentioned, face recognition is one of the best ways of identifying a person.[27]

3.1. What about biometric data?

According to Article 4(14) GDPR, '"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'. Indeed, the facial image of a Kodak's hyper-realistic Metaverse avatar is not a proper facial image but the facial image of a photorealistic representation of a person. However, if it fits the technical requirements stated within the abovementioned definition, Kodak's hyper-realistic Metaverse avatars should be considered biometric special categories of personal data.

First, biometric data must be personal data. This implies that before being allowed to legally be referred to as 'biometric', this kind of data must meet the requirements that apply to all other categories of personal data. The cutoff point for determining an individual's identity is still low: the person simply has to be made recognizable, not necessarily identified. Second, technical processing is mentioned in the statutory definition of biometric data. Other than stating that the goal of the processing should be to uniquely identify a person, it does not define what is meant by 'specific technical processing'. Third, the concept of biometric data is related to the criterion 'relating to the physical, physiological, or behavioural characteristics of a natural person'. Such

22 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

23 Lee A. Bygrave and Luca Tosoni, 'Article 4(1). Personal data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), available at: https://doi.org/10.1093/oso/9780198826491.003.0007 (accessed 9 May 2024).

24 C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779.

25 Article 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy replaced by the European Data Protection Board effective on 25 May 2018 (entry into application of the GDPR).

26 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (adopted on 20 June 12).

27 Lisa Bock, *Identity Management with Biometrics: Explore the Latest Innovative Solutions to Provide Secure Identification and Authentication* (Packt Publishing, 2020).

a reference recognizes the wide range of observable human traits that may be utilized for biometric identification. These traits include physiological and anatomical features (like a fingerprint, face or iris) as well as behavioural traits (like speech, movement or signature). Finally, the term 'allowing or confirming the unique identification of that individual' refers to the uses of biometric traits, which are the source of biometric data. Additionally, it establishes the level of identification required for biometric data as a subset of personal data. It expands upon knowledge of the distinctions between identification in a data protection environment and biometric identification.[28] I argue that hyper-realistic Metaverse avatars indeed fulfil the biometric data definition. First, as discussed in the previous section, they are personal data since they make a person recognizable. Second, the process of creating an avatar entails precisely a specific technical processing (as described within Section 2) to generate an avatar, a digital representation that allows to uniquely identify a Metaverse user from others. Third, the hyper-realistic avatar not only allows but also is created to digitally represent a person, from their physical (i.e. face) to their behavioural characteristics (i.e. speech and movement). Fourth, as previously mentioned, hyper-realistic Metaverse avatars contain extremely accurate information about a person's face, which would allow their unique identification.

Finally, biometric data are not the only special categories of personal data. Data revealing race or ethnic origin and/or health data will also benefit from the special regime of Article 9 GDPR. In this regard, Metaverse avatars showing, for instance, skin colour (potentially one attribute of race) or health conditions such as a disability could also be considered special categories of data.

3.2. Data governance of hyper-realistic Metaverse avatars

If we consider Kodak's hyper-realistic Metaverse avatars as personal data, special categories of data and/or biometric data, the legal regime applicable to such avatars will be that of the GDPR. In this regard, to comply with the GDPR and therefore be lawful under EU law, the data processing operations necessary to generate and manage Kodak's hyper-realistic Metaverse avatars will need to follow the following principles and rules:

3.2.1. Lawful basis for processing (Articles 6 and 9(2) GDPR)

Before conducting any kind of processing activity and thus applying the principles that will be discussed within the following sections, compliance with a legal base for lawful personal data processing is required. Depending on the categories of data that we are discussing, we could find such bases in Article 6 GDPR (personal data) and Article 6 plus concurrence of one of the exceptions of Article 9(2) GDPR (special categories of data). In the case of Kodak's hyper-realistic Metaverse avatars, I think consent will be the most likely base for lawful data processing. In the past, Big Tech companies have turned to other lawful bases for data processing, such as legitimate interest (Article 6(1)(f) GDPR) or performance of a contract (Article 6(1)(b) GDPR). However, both the legitimate interest and performance of a contract lawful basis would be excluded in the case of processing of special categories of personal data since they are not contemplated within the exceptions of Article 9(2) GDPR. But even if we consider that we are just processing personal data and not special categories of data, Data Protection Authorities have been very strict about the use of the legitimate interest lawful base by Big Tech companies, especially concerning targeted advertising.[29]

According to Article 4(11) GDPR, '"consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Further, Articles 7 and 8 GDPR establish the conditions for consent and the conditions applicable to a child's consent concerning information society services. Since children and young adults are one of the main target users of Metaverse environments, it is also likely to assume that some of them would encounter at some point the possibility of creating a hyper-realistic avatar. In this case, adequate safeguards should be implemented to ensure that young Metaverse users and their guardians are fully aware of what they are consenting to by creating a hyper-realistic Metaverse avatar. But also for adults, consent should be informed about all the potential risks that such avatars could entail, such as identity theft, for instance, via the

28 Catherine Jasserand, 'Legal nature of biometric data: from generic personal data to sensitive data' (2016) 2 European Data Protection Law Review (EDPL) 297, available at: https://heinonline.org/HOL/P?h=hein.journals/edpl2&i=323 (accessed 2 July 2023).

29 Oreste Pollicino and Giovanni De Gregorio, 'European data protection and social media: the quest for consistency in the internal market' (Medialaws, February 6 2023).

use of biometric features present within the avatar such as the face image to unlock certain biometric authentication services. Consent can be also revoked any time by the data subject.

Regarding the processing of special categories of personal data, Article 9 requires 'explicit' consent. According to Article 29 Working Party, '[t]he term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent'.[30] This could mean a written statement signed by the data subject but also, 'in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature'.[31] Considering that hyper-realistic avatars entail the replication of one's physical appearance plus other biometric traits, such as voice cloning in a digital environment, consent by the data subject should be explicit. It should also be granular since hyper-realistic avatars can have different levels of personalization and be used in different (and even interoperable) Metaverse environments.

Informed consent, if properly implemented following the GDPR requirements, is a strong tool in the hands of data subjects. Because of this, I do not think a more developed and sophisticated form of consent is needed to generate and release such a digital replica. However, the key is indeed in the implementation and enforcement aspects. This could also be seen in the example of dark patterns. According to the Spanish Data Protection Authority,

> The term dark patterns refers to user interfaces and user experience implementations intended to influence people's behaviour and decisions when interacting with websites, apps and social networks, so that they make decisions that are potentially detrimental to the protection of their personal data.[32]

Due to the structure and appearance of the consent form, it may be extremely easy to access personal information and/or very difficult to refuse consent if the opt-in option is set by default. The same might occur if the data subject finds it difficult or burdensome to accept the opt-out choice. In such cases, the privacy policy of Metaverse environments regarding the creation of hyper-realistic avatars should be carefully monitored to avoid this kind of practice, particularly when children and young adults might be affected by it.

3.2.2. Purpose limitation (Article 5(1)(b) GDPR)

Before using personal data, it is important to define the goal for collecting and processing the data, while also considering the threats to people's fundamental rights and freedoms. In this case, it should be specified which data are necessary for the avatar's creation and how it will be used. Further, the data collected and processed with the purpose of the creation and functioning of the avatar should be not employed for other purposes for which consent was not collected such as targeted advertisement. Finally, whenever feasible, data subjects should be able to choose between different modalities of an application with numerous features, especially if one or more involve biometric data processing. Therefore, hyper-realistic avatars should not be the only method of digital representation within Metaverse environments. Other alternatives, such as random avatars, should be provided for those users who do not wish to be hyper-realistically represented.

3.2.3. Data minimization (Article 5(1)(c) GDPR)

Personal data may contain unnecessary information; therefore, the data controller must enforce the principle of data minimization. This means that just the essential information is available, rather than everything. Further, the data controller should guarantee that the default setting supports data protection without the need for active enforcement. In this case, the granularity of avatars should play a key role. Users should be able to decide the accuracy of their avatars regarding certain aspects such as information that reveals health data, or whether they also want voice cloning functionalities applied as well as the interoperability of such avatars to be used within other Metaverse platforms.

3.2.4. Proportionality

The principle of proportionality is the general legal notion behind the principle of data minimization. The use of biometrics poses the problem of the proportionality of each type of processed personal data concerning the purpose for which they are processed. Because biometric data can only be used if it is suitable, necessary and not excessive, it requires a rigorous evaluation of the need and proportionality of the processed personal data, as well as if the intended goal might be fulfilled in a less invasive manner.

30 Article 29 Working Party Guidelines on consent under Regulation 2016/679 (adopted on 28 November 2017 and revised on 10 April 2018) p. 18.

31 Ibid.

32 Agencia Espanola de Proteccion de Datos, *Metaverso y privacidad* (September 2022), available at: https://www.aepd.es/prensa-y-comunicacion/blog/metaverso-y-privacidad.

When assessing the proportionality of a proposed biometric data processing, it is important to examine whether it is necessary to address a specific demand, rather than just being convenient or cost-effective. The system's likelihood of being successful in fulfilling that need while taking into account the particulars of the biometric technology that will be employed is a second consideration. Whether the consequent loss of privacy is commensurate with any projected advantage is a third factor. The loss of privacy is inappropriate if the benefit is relatively little, like slight cost savings or an increase in convenience. Examining whether a less invasive method may accomplish the goal is the fourth factor in determining if biometric data processing is adequate. In this regard, it should be considered whether hyper-realistic Metaverse avatars represent a necessary development within the enjoyment of Metaverse experiences. Accordingly, a balancing operation should be conducted to discern whether the technological advantage they provide justifies the potential interference with fundamental rights, particularly privacy and data protection. Particularly, whether the hyper-realistic nature of new avatars introduces an enhancement within the Metaverse enjoyment or whether it is just another 'cool' feature to add, should be carefully balanced.

3.2.5. Storage limitation (Article 5(1)(e) GDPR)

The controller should establish a storage period that is no more than what is required for the purposes for which the data were gathered or for which they are subsequently processed. After that appropriate amount of time, the controller is required to make sure that the data, or profiles created from such data, are completely erased. Along this line, once Metaverse users decide not to participate more in virtual environments, if they are expelled from some communities or if the communities close, all data should be immediately deleted, including their hyper-realistic Metaverse avatars. Also, all data that are required to create the hyper-realistic Metaverse avatar, but not necessary once the creation process has finished, should be deleted as well.

3.2.6. Transparency and information duties (Article 5(1)(a) and Chapter III GDPR)

Data subjects must be informed about the acquisition and/or use of their personal and biometric data under the fairness and transparency principles. To comply with the data subjects' rights, the data controller must ensure that the data subjects are sufficiently informed about the essential components of the processing, including the controller's identity; the purposes of the processing; the type of data; the duration of the processing; the subjects' rights to access, rectify or cancel their data; the right to withdraw consent; and the recipients or categories of recipients to whom the data are disclosed. This takes us to the privacy policies of hyper-realistic Metaverse avatars. Such policies should extensively but comprehensively inform potential data subjects of the data processing operations encompassing the creation of hyper-realistic Metaverse avatars.

3.2.7. Data security (Article 32 GDPR)

Data controllers are required to put in place the necessary organizational and technical safeguards to prevent any unauthorized processing, accidental or unlawful destruction, loss, modification, disclosure or access, as well as against any other unlawful forms of processing. System designers must collaborate with relevant security specialists to effectively address security vulnerabilities, particularly in Metaverse environments connected to the Internet. Especially considering the sensitive nature of special categories of personal data.

3.2.8. Data transfers (Chapter V GDPR)

Cross-border data transfers to countries outside the European Economic Area (EEA) or to international organizations are critical components of the Metaverse infrastructure since most of the companies offering 'Metaverses', including Meta, are located outside the European Union, particularly the US.

The export of personal data from the EEA to third countries must comply with a set of criteria and requirements outlined in Chapter V of the GDPR. Aside from adhering to the rules outlined in Chapter V, transferring personal data to a non-EEA country or international organization necessitates adhering to the GDPR basic processing principles, which include having an appropriate legal basis for processing, implementing the necessary security measures and only processing the personal data required for the specific processing activity. According to the GDPR, there are two basic ways to transmit data outside the EEA. The first one involves transfers based on an adequacy judgement (Article 45 GDPR). According to an evaluation by the European Commission, the third country or international organization in question must have an 'equivalent level of data protection' to that prevailing in the EEA region.[33] The second method involves

33 So far the EC has adopted adequacy decisions for Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (commercial organizations participating in the EU-US Data Privacy Framework) and Uruguay. See https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en.

transfers subject to sufficient protections (Article 46 GDPR). The 'appropriate safeguards' that may be used to transfer personal data to non-EEA countries in the absence of adequacy decisions can be provided by the various transfer tools listed in Article 46(2) GDPR: standard data protection clauses (SCCs), binding corporate rules (BCRs), codes of conduct, certification mechanisms and *ad hoc* contractual clauses. Additionally, the GDPR allows for data transfers based on exceptions (Article 49 GDPR). These transfers are seen as exceptional and may be used in the following situations: when made with the express consent of the individual; when required for the execution of a contract between the individual and the organization, or for pre-contractual actions taken at the individual's request; when required for the execution of a contract made in the individual's best interests between the data controller and another party; when required for significant public interest considerations; when required for the establishment, exercise or defence of legal claims; when required to safeguard the vital interests of the concerned individual or other parties in cases where the concerned individual is physically or legally unable to give consent; or when derived from a register that is intended to provide public information under EU law or national law of an EEA country (and which is accessible for public consultation by anyone with a legitimate interest in viewing the register). Along these lines, international data transfers containing personal data related to hyper-realistic Metaverse avatars should comply with the GDPR and also with the specific safeguards established within Chapter V. Considering that it is most likely that the avatar creation process takes place mostly in countries outside the EU, considering the state of the art of the technology and the fact that the biggest Metaverse developers are located outside the EU, constant and consistent compliance with data transfers provisions should be carefully monitored. As discussed in this section, compliance of hyper-realistic Metaverse avatars with the GDPR is not a trivial task. Therefore, the existence of privacy-enhancing technologies and solutions might come in handy in this respect. Because of this, the next section will discuss the use of blockchain technology for the data governance of hyper-realistic Metaverse avatars.

4. The use of blockchain technology for Metaverse avatar personal data governance

In the above-mentioned landscape of the data protection challenges raised by the existence of hyper-realistic Metaverse avatars, blockchain technology emerges as a privacy-enhancing solution for the personal data governance of such avatars. Apart from the inherent advantages of blockchain technology, such as its decentralized, immutable and transparent nature, blockchain might help prevent identity theft, a possibility arising from the particular nature of hyper-realistic Metaverse avatars as opposed to traditional avatars. In a world moving more and more towards digital identity systems[34] and biometric authentication and verification solutions,[35] hyper-realistic Metaverse avatars could open a door, for instance, to unlawful face template[36] processing.

According to Finck, 'a blockchain is a shared and synchronized digital database that is maintained by an algorithm and stored on multiple nodes (the computers that store a local version of the distributed ledger). Blockchains can be imagined as a peer-to-peer network, with the nodes serving as the different peers'.[37] To provide users with the best experiences possible, the Metaverse processes enormous amounts of personal data. Users might have total control over their personal data thanks to blockchain's consensus, authentication and access control methods, which protect users' privacy. Finally, blockchain enhances data security in the Metaverse in line with Article 32 GDPR by utilizing hash functions and asymmetric key encryption. However, when one thinks about the possibility of introducing blockchain technology to enhance the data governance of hyper-realistic Metaverse avatars, the infrastructural costs should be also considered. First, the typical costs of blockchain development for 2024 are estimated between $15,000 and $50,000.[38] Second, the environmental impact of blockchain technology has been widely criticized. According to Clarke, '[b]lockchain technology has a significant carbon footprint due to its energy-intensive process of verifying transactions and creating new blocks on the blockchain. The energy consumption of blockchain

34 '2023: the year digital identities go mainstream', available at: https://www.forbes.com/sites/forbestechcouncil/2023/03/24/2023-the-year-digital-identities-go-mainstream/?sh=1630c57244b5 (accessed 16 May 2024).

35 Anil K. Jain, Debayan Deb and Joshua J. Engelsma, 'Biometrics: trust, but verify' (2022) 4 IEEE Transactions on Biometrics, Behavior, and Identity Science 303, available at: https://ieeexplore.ieee.org/document/9581287 (accessed 16 May 2024).

36 According to the European Data Protection Board, a (face) template is 'a digital representation of distinct characteristics of [a] face' in European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 2.0 (adopted on 26 April 2023).

37 Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 2018) 6.

38 Suffescom Solutions, 'How much does blockchain development cost in 2024?' (September 30, 2024), available at: https://www.suffescom.com/blog/blockchain-development-cost#:~:text=The%20blockchain%20development%20cost%20can,your%20blockchain%20project%20will%20cost (accessed 18 December 2024).

technology results in significant greenhouse gas emissions, which contribute to climate change'.[39]

Another aspect that should be considered is the difference between private and public blockchains. Public blockchains are accessible to everybody and provide some level of anonymity. Private blockchains, on the other hand, only provide access to a limited number of people and institutions.[40] While public blockchains offer transparency, decentralization and accessibility, private blockchains allow for better control, privacy and security. In the specific case of hyper-realistic Metaverse avatars, it could be considered to have a private blockchain accessible for all the users and deployers of a specific Metaverse space. This might help to enhance privacy, data protection and data security.

Data security is crucial, since the room for illegal activities within Metaverse environments is vast. Some examples can include hacking, identity theft, deepfake, exploitation of security flaws in virtual environments and financial fraud. These will be especially relevant in the case of hyper-realistic Metaverse avatars. The amount of personal and, as discussed in the previous section, biometric data, can make hacking or data breaches particularly dangerous. Also because biometric data, unlike passwords or bank account numbers, cannot be erased. Other crimes might include cyberstalking, harassment, disruptive behaviour, discrimination, intimidation or deception. Figure 2 shows an overview of potential harms in and through the Metaverse.

The advantages of blockchain for the personal data governance of hyper-realistic Metaverse avatars will be four-fold. First, the use of blockchain technology will facilitate the acquisition of personal data in the Metaverse for applications such as social networking. Blockchain's distributed ledger will make it possible to validate transaction records and follow personal data across the Metaverse.[41] Since every action on a blockchain is tracked as a transaction, and each block includes information, a timestamp and a cryptographic hash of the block, personal data in a block cannot be changed without also changing the other blocks. Any block can be used to extract personal data that are impervious to manipulation. There is very little possibility of producing a duplicate block, guaranteeing that there is no duplication during the data collection procedure. Thus, the personal data obtained by blockchain-enabled acquisition systems in the Metaverse will be trustworthy since each block in the blockchain is approved. Again, this will help enhance personal data security in line with the requirements set up by Article 32 GDPR.

Second, the Metaverse storage will be unchangeable as a new block is generated for each transaction. As a result, personal data are preserved along the chain as a duplicate of the original blocks, increasing personal data transparency and dependability, in line with the transparency principle of the GDPR. Third, according to the literature, to guarantee communication across virtual worlds inside the Metaverse, a cross-chain protocol is an ideal remedy.[42] This makes it possible for items like avatars to be traded across virtual worlds. This protocol will lay the foundation for the Metaverse to be widely adopted. Cross-blockchain technology will make it possible for virtual worlds to communicate with one another, doing away with the necessity for middlemen in the Metaverse. Thus, applications and users will find it easier to connect in the Metaverse thanks to blockchain.

By enabling the usage of private and public keys, blockchain technology allows Metaverse users to take more ownership of their personal data and exert control over it. Third-party intermediaries are not allowed to get or misuse personal data from other parties in the blockchain-enabled metaverse. When it comes to personal information stored in the blockchain-enabled Metaverse, personal data owners will have control over the circumstances surrounding when and how an outside party can access their personal data. According to Finck, public keys are 'a string of letters and numbers that allows for the pseudonymous identification of a natural or legal person for transactional or communication purposes'.[43] Therefore, the information remains anonymized by rendering the keys anonymous. Blockchain ledgers come with an audit trail as standard, guaranteeing the consistency and completeness of transactions in the Metaverse. Zero-knowledge proof adoption on the blockchain safeguards users' privacy and preserves ownership of their 'digital' belongings including their avatars, while providing easy access to the identification of crucial personal data in the Metaverse. Through the use of blockchain technology and zero-knowledge proofs, people can show Metaverse apps that certain information about them is

39 Anthony Clarke, 'The environmental impact of blockchain technology | Nasdaq' (30 May 2023), available at: https://www.nasdaq.com/articles/the-environmental-impact-of-blockchain-technology (accessed 18 December 2024).

40 Elias Strehle, 'Public versus private blockchains' *BRL Working Paper, Blockchain Research Lab*, Tech. Rep. (2020).

41 Natarajan Deepa and others, 'A survey on blockchain for big data: approaches, opportunities, and future directions' (5 February 2021), available at: http://arxiv.org/abs/2009.00858 (accessed 16 May 2024).

42 Rafael Belchior and others, 'A survey on blockchain interoperability: past, present, and future trends' (2021) 54 ACM Computing Surveys 168:1, available at: https://dl.acm.org/doi/10.1145/3471140 (accessed 16 May 2024).

43 Michèle Finck, 'Blockchains and data protection in the European Union' (2018) 4 European Data Protection Law Review 12, 17, available at: https://edpl.lexxion.eu/article/EDPL/2018/1/6 (accessed 24 June 2024).

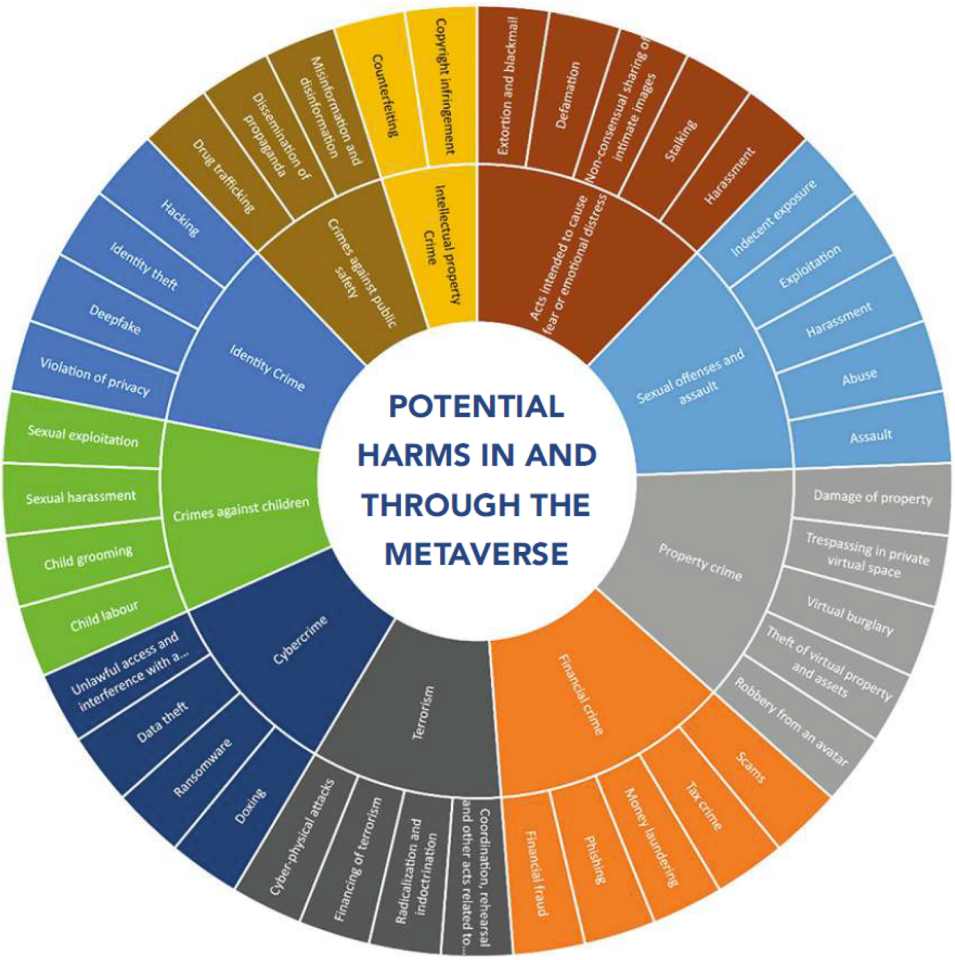

Figure 2 Crimes in the Metaverse

Source: Interpol, Metaverse: A Law Enforcement Perspective Use Cases, Crime, Forensics, Investigation, and Governance, White Paper January 2024.

true without having to provide that information.[44] To sum up, the use of blockchain might allow the transparency of personal data processing operations in line with the GDPR's transparency principle, maintaining the anonymity of the Metaverse users at the same time. This is important since some actors might question the potential trade-off between transparency and confidentiality/privacy of the personal data stored within the blockchain. However, the anonymization of the personal data via the key's anonymization will ensure the protection of the data subject. If the data subject decides to willingly share their key, implicit consent could be argued from this, thus ensuring compliance with the GDPR's provisions. Further, because of blockchain's decentralized character, the lack of intermediaries will reduce the potential for personal data breaches and access to third parties will be highly restricted, incrementing the security of the personal data processing operations, in line with the GDPR's data security provisions.

Finally, it should be considered that blockchain, according to the scholarship, poses some caveats from a privacy and data protection perspective.[45] For instance, there is the widely discussed lack of a 'right to be forgotten' when using blockchain technology for the processing of personal data.[46] This might collide with the storage limitation and data minimization principles mentioned

44 Johannes Sedlmeir, Fabiane Völter and Jens Strüker, 'The next stage of Green Electricity Labeling: using zero-knowledge proofs for blockchain-based certificates of origin and use' (2022) 1 ACM SIGEnergy Energy Informatics Review 20, available at: https://doi.org/10.1145/3508467.3508470 (accessed 16 May 2024).

45 Rahime Belen-Saglam and others, 'A systematic literature review of the tension between the GDPR and Public blockchain systems – ScienceDirect', available at: https://www.sciencedirect.com/science/article/pii/S2096720923000040 (accessed 24 June 2024).

46 Donatella Casaburo, 'Distributed ledger technologies and GDPR's right to be forgotten: can they get along?' (*CiTiP blog*, 11 January 2022), available at: https://www.law.kuleuven.be/citip/blog/distributed-ledger-technologies-and-gdprs-right-to-be-forgotten/ (accessed 24 June 2024).

in the previous section. In this case, a balancing operation must be done to weigh the privacy-friendly features that the use of blockchain might entail for the data governance of avatars, with the abovementioned caveats, including the infrastructural and environmental costs. In the end, the decision that entails a greater benefit for the data subject/avatar owner should be taken.

5. Conclusion

This paper has discussed the data governance regime applicable to hyper-realistic Metaverse avatars. Taking as a role model Kodak's hyper-realistic Metaverse avatars presented by Mark Zuckerberg in a podcast interview in September 2023, the paper has discussed the role of avatars within Metaverse environments and the features of hyper-realistic Metaverse avatars, which make them worth attention, particularly from a data governance perspective. In this regard, the paper has argued that hyper-realistic Metaverse avatars can be considered personal data and further special categories of personal data such as biometric data, data revealing race and/or health data. Consequently, the application of data governance principles from the GDPR is crucial to ensure compliance of hyper-realistic Metaverse avatars with the EU data protection regime. Some of these principles regard purpose limitation, data minimization, proportionality, storage limitation, transparency and accountability. Further, the lawful ground for the personal data processing and whether any of the exceptions from Article 9(2) GDPR are applicable were also reviewed, being consent the most likely basis for lawful personal data processing in the context of hyper-realistic Metaverse avatars. Then, the rights of the data subject such as the right to access and the information duties of the data controller were discussed regarding a compliant data governance of Metaverse avatars. Lastly, two important questions, data security and the legal regime applicable to data transfers were also considered due to their particular relevance when dealing with hyper-realistic Metaverse avatars. Considering the nature of the data contained within hyper-realistic Metaverse avatars and the fact that many Metaverse companies are located outside the EU, particularly in the US, data security requirements and compliance with the data transfer provisions of the GDPR will be crucial. Finally, the paper has proposed the use of blockchain technology within four lines of action as a privacy-enhancing technology regarding the data governance of hyper-realistic Metaverse avatars: to extract personal data from social media with data security guarantees, therefore preventing identity theft; to increase the transparency of the information processed without compromising privacy and confidentiality; to be interoperable eliminating the need for intermediaries and to allow Metaverse users to take ownership of their personal data and exert control over it.