# International: The end-user and its avatar - Data integrity risks and ethical challenges in the metaverse - Part one

As the metaverse is being accessed by means of an avatar and, in some cases, by means of technologically advanced devices, the avatar and these devices can be regarded as the 'keys' to the metaverse environment. However, this poses specific data integrity risks for the end-user's personal data, as well as privacy-related ethical challenges related to specific categories of end-users, such as children[1].

Therefore, in part one of this two-part Insight series, Danique Knibbeler, Max Mohrmann, and Sarah Zadeh, from NautaDutilh N.V., focus on the data integrity risks and ethical challenges related to the end-user and its avatar and discuss potential remedies in this regard.

## Context

The article EU: Privacy and security concerns in the metaverse describes the current and upcoming data regulations in the metaverse on a high-level and explores multiple privacy and security concerns. One of the concerns discussed were the multiple risks that relate to the end-users, and the extensive amount of personal data of the end-users that is being processed by multiple parties within the metaverse.

## End-users and their avatars

One of the technical characteristics of the metaverse is the concept of interoperability, which allows different devices, platforms, and environments to interact with each other and exchange (personal) data[2]. The purpose of connecting these different devices, platforms, and environments is to offer an immersive virtual experience to the end-user that wishes to participate in the metaverse.

Once the end-user has connected with, or logged on to, a specific metaverse platform, the end-user is able to engage in different virtual activities, connect with (third-party) devices, platforms, and environments, and interact with other end-users by means of an avatar. In our opinion, the avatar can be regarded as the 'protagonist' and thus 'the main subject' in the metaverse, for it is the avatar

that serves as a virtual interconnection between the end-user and this virtual and immersive space, which is often accessed via physical digital devices, such as VR-goggles.

In our view, an avatar is therefore best regarded as the virtual embodiment of the end-user, whose appearance and characteristics can be further customised and personalised. In addition, the end-user can purchase virtual assets, such as clothing and real estate, or virtual services, such as entrance tickets for virtual concerts, which can be used by the avatar. The avatar does not have to be a direct reflection of, or bear physical resemblance to, the end-user. The end-user can also choose to deploy the avatar as an alternative self; it can thus also be viewed as a 'virtual alter ego'.

## Data integrity risks and recommendations

Due to the interoperability between different devices, environments, and platforms, extensive amounts of personal data are being shared with different third parties in the metaverse[3]. Although attention should be given to potential technical weaknesses and the appropriate technical measures that could be taken to prevent potential cyber incidents, sufficient consideration should also be given to potential actions of the end-user in the metaverse. Human errors are a contributing factor in over 95% of all cybersecurity incidents[4], and therefore, also in the metaverse, the end-user may potentially be the weakest link.

## Risks: identity theft, fraud, and impersonation attacks

When the accounts of the avatar and the platforms on which they engage are inadequately secured, increasing identity-related security risks may occur[5]. By performing phishing attacks or by hacking into the systems and the associated devices, hackers can try to steal or duplicate the identity of the avatar and commit identity fraud by seizing the account(s) of the avatar[6]. This means that not only the virtual assets, wallets, and funds connected to the avatar's account can be stolen, but also the social connections and personal data, which in the most serious case may also include the end-user's health data, if wearables are used and biometric data for identification or authentication purposes and if advanced VR goggles are used. Passwords and usernames can be reset, but biometric data cannot be reset; biometrics are connected with the individual and once exposed, the individual becomes an easy target for multiple cyber attacks, such as identity theft.

Once identity theft has occurred, hackers are able to further misuse the avatar and its account(s), by carrying out impersonation attacks, for example by misusing the existing avatar and its account(s), or by creating other avatars or replicas based on the end-users' biometric data and other personal data[7]. These avatars may be used to send spam to social connections within and outside the metaverse, but also to commit phishing attacks or fraud.

## Recommendations

In our previous article, we distinguished two different types of metaverses, namely a centralised blockchain-based metaverse (e.g. Earth2) or a decentralised blockchain-based metaverse (e.g. Decentraland, The Sandbox). We chose to coin such blockchain-based metaverses as 'advanced metaverses' - this in contrast to centralised metaverses, which are not blockchain-based (e.g. Second Life, Grand Theft Auto Online), which we chose to coin as a 'traditional metaverses'. It can be argued that implementing robust and adequate technical standards and measures, such as cross-platform identity authentication and account verification, and building this on a decentralised blockchain network, reduces the risk of cyber attacks and increases the level of cyber resilience[8]. In this regard, decentralised advanced metaverses may have an 'extra edge' over traditional metaverses. However, cross-platform development on a decentralised blockchain-based network will also bring other challenges, such as the increased exchange of personal data of end-users between the associated platforms and environments[9].

## Privacy-related ethical challenges and recommendations

Besides data integrity and security issues in relation to the avatar, which can be (partially) mitigated by implementing adequate technical and organisational measures, the individual platforms, devices, and environments must take into account that the metaverse may pose privacy-related ethical challenges in relation to the end-user and its avatar, and thus careful consideration is required prior to any processing activities.

## Challenges: harmful content and mental health issues

Uncontrolled use of virtual space can lead to exposure to harmful content, but also spreading misinformation. Even though the spreading of, and exposure to, harmful content and misinformation are no new phenomena within the digital realm, as such content can be easily shared online, which poses further challenges in the metaverse.

Due to the immersive nature of the metaverse, the amount of personal data that is being shared, and the possibility for vulnerable individuals, such as minors, to easily access the metaverse and interact with others, the metaverse may pose risks to vulnerable individuals[10]. The European Parliamentary Research Service stresses that, in the metaverse, augmented and virtual reality will create new content moderation challenges, for example, in relation to inappropriate actions and online harassment by other end-users, and misinformation, disinformation, and defamatory content, which have been generated by using augmented reality[11]. As vulnerable individuals, such as minors, but also individuals that experience mental health issues, are more easily influenced and may be harmed by such content and actions, special attention is required in relation to

implementing organisational and technical measures to offer certain protections for vulnerable individuals in the metaverse.

## Recommendations

Taking specific appropriate technical and organisational measures in relation to the metaverse may become market practice based on EU-standards, such as the 'EU strategy for a better internet for children', or may even become mandatory based on new legal frameworks and legislative proposals that have been introduced by the European Commission, such as:

- the Digital Services Act ('DSA'), which aims at modernising Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services in Particular Electronic Commerce in the Internal Market ('the e-Commerce Directive') regarding illegal content, transparent advertising, and disinformation;
- the Proposal for a Regulation of the European Parliament and of the COuncil on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ('the Draft Cyber Resilience Act'), which will introduce mandatory cybersecurity requirements for products with 'digital elements'[12];
- the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI ('the Draft AI Act')[13]; and
- the Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence 2022/0303 (COD) ('the AI Liability Directive'), which introduces uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of artificial intelligence ('AI') systems[14].

Therefore, to mitigate the risk of the spreading harmful content and to reduce the risk of vulnerable individuals from being adversely affected, it is recommended that platforms, device manufactures, and software developers think of appropriate strategies and policies in this regard, and implement clear policies and notices for the end-users, by looking into technical possibilities to detect and block harmful content, verifying end-users age, and avoiding the set-up of fake accounts.

## Conclusion

In this article, we have addressed multiple data integrity risks, such as identity theft, fraud, and impersonation attacks, and given an overview over privacy-related ethical challenges that relate to the end-user and its avatar. Due to the interoperability and interconnection of multiple platforms, environments, and devices in the metaverse, and the central role that the avatar plays in this regard, it is recommended that platforms, device manufacturers, and software developers implement appropriate technical and organisational measures to further safeguard (vulnerable) individuals and strengthen the integrity of its systems. Based on the upcoming European legislative proposals, such measures may even become mandatory.

**Danique Knibbeler | Associate**
Danique.Knibbeler@nautadutilh.com

**Max Mohrmann | Associate**
Max.Mohrmann@nautadutilh.com

**Sarah Zadeh | Associate**
Sarah.Zadeh@nautadutilh.com

NautaDutilh N.V., Amsterdam

1. See at: https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf
2. See at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
3. See at: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf
4. See at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
5. See at: https://arxiv.org/pdf/2203.02662.pdf
6. See at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
7. See at: https://arxiv.org/pdf/2203.02662.pdf
8. Ibid.
9. See at: https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf
10. Ibid.
11. See at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
12. Available for download at: https://ec.europa.eu/newsroom/dae/redirection/document/89543
13. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
14. Available at: https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf