MetaverseUA Chair

Academic Chair for the Responsible Development of the Metaverse

Ubiquity of personal data through the Virtual Worlds

Proceedings of the International Congress Towards a Responsible Development of the Metaverse, 13-1 4 June 2024, Alicante

Francisco Javier López Guzmán
University of Alicante

catedrametaverso.ua.es

Universitat d'Alacant
Universidad de Alicante

The Chair for the Responsible Development of the Metaverse (MetaverseUA Chair) was created by the University of Alicante (Spain) and financed by Meta Platforms under its XR Program and Research Funds. The Program aims at supporting academic and independent research across Europe into metaverse issues and opportunities. The MetaverseUA Chair is a member of the European Metaverse Research Network. Like all our work, this report has been produced completely independently. The ideas expressed in this paper are the sole responsibility of the author.

How to cite this paper:

López-Guzmán, F.J., `Ubiquity of personal data through the Virtual Worlds´ (2024) *Proceedings of the International Congress Towards a Responsible Development of the Metaverse*, Alicante, 13-14 June, 2024.

Abstract

Every time a user logs into a virtual world, his personal data is processed. This processing is done for the sake of the service that he is enjoying. But also for the profit of the company who hosts this virtual world. One important side for the development of this service (and the maximisation of this profit) is the international flow of these personal data. Companies offer access to the Metaverse all around the world. Similarly to the more traditional digital services such as social media, these companies are territorially based in specific countries, but offer their services all around the world. They have an interest in the free flow of this personal data. However, they are also subject to privacy regulations wherever they offer their services. The extra-territorial component of privacy laws poses many questions for the Metaverse. Such as data localisation, anonymisation of the data, accountability, cybersecurity…The objective of this article is to point at the main challenges that the Metaverse poses to the territorial scope of privacy laws. It also sets a comparison with their previous solutions (or attempts) in similar digital environments.

Keywords: Data-driven Metaverse business model, traditional social media, ubiquity of personal data, virtual worlds as a global service, Open Internet

Table of Contents

1. Introduction: the data-driven business model of the Metaverse

The current first approach to the Metaverse by the general public is done through video games. The industry of virtual entertainment has been the first one in developing an interest in this concept. Traditional video games were very advanced in terms of graphic design. The first video game is considered to be *Spacewar!*, created in 1962[1]. Or, at least, the first video game issued outside of a laboratory.[2] Very basic graphics, usually showing in black and white. Later, the boost of the entertainment industry brought pictures full of colours and action, such as *Sonic the Hedgehog* or *Metal Slug* series.

Those were the days of discovery through the screens. Hardware equipment has been evolving also through time. From the days of the first world-wide commercialised gaming console (*Magnabox Odyssey*, 1972[3]), going through famous equipment such as 1990's *Atari 2600* or *Nintendo 64*, to the current hyper-connected machines *Play Station 5* or *XBOX 365*. Nowadays it is also possible to obtain a similar gaming experience simply by playing using a regular laptop.

We define traditional videogames as requiring specific traditional hardware, in opposition to those developed in the Metaverse. They are nowadays very detailed, with hyper-realistic images such as *Red Dead Redemption* and *EA Sports FIFA*, or cartoon-like worlds full of possibilities like *Minecraft*. But still not immersive enough, since the interaction in the game requires motion on hardware (such as remote controllers, joysticks or later touchable screens) and visual experience through a screen.

Traditional video games are full experiences that may distract our mind from our everyday lives. However, they lack a number of elements to fully take our attention from the physical world. Those are:

- The immersion. Traditional video-games are still perceived in our senses through the hardware equipment abovementioned. There is a limit in the immersion that a screen may create. Although a screen may be very engaging, there is a clear limit in the experience of its use, compared to the equipment needed to interact in the Metaverse, such as Virtual Reality (VR) glasses. Current time spent through screens vary sensibly between countries, but it is set in 7 hours and 4 minutes per day for the United States of America[4] and 5 hours 42 minutes for Spain[5]. This is a relatively high amount, but still limited if compared to the full potential of the Metaverse.
- The script. Most traditional videogames are scripted. When playing them, we follow a pre-set story. Perhaps with multiple options, or tiny variations depending on our interaction. But mostly pre-defined by a team of scriptwriters. Human minds that foresee the variation and possible interactions within the game and the players. Reality cannot withstand the script, and it is therefore a limitation of traditional gaming compared to the virtual worlds.

---

[1] Graetz JM, 'The Origin of Spacewar' [1981] Creative Computing magazine <https://www.wheels.org/spacewar/creative/SpacewarOrigin.html> accessed 1 June 2024.

[2] Brookhaven National Laboratory, 'History:The First Video Game?' https://www.bnl.gov/about/history/firstvideo.php accessed 1 June 2024.

[3] Ralph H Baer, *Videogames: In the Beginning* (Rolenta Press 2005). 52–59.

[4] Simon Kemp, 'Digital 2024: Global Overview Report' (DataReportal, 31 January 2024) <https://datareportal.com/reports/digital-2024-global-overview-report> accessed 1 June 2024.

[5] Matthew A Christensen and others, 'Direct Measurements of Smartphone Screen-Time: Relationships with Demographics and Sleep' (2016) 11 PLOS ONE.

The Metaverse does not have these limits. That is why it is a means to scale the gaming experience. Besides, the elements of liberty (non-script) and immersion are key to draw other experiences of real life to the virtual worlds, such as professional activity, arts and sporting events (not electronic-sports, already present in the traditional gaming).

Why introducing these concepts in a legal scientific paper? Because they are the key elements that the Metaverse is expanding for human interactions. They are needed for the escalation of the Metaverse, and actively pursued by the corporations which exploit the virtual worlds. Thus, in order to attract more users to these platforms, domain the digital landscape and increase their economic profit. And they are the germ of activities with global legal implications, such as the processing of personal data in the virtual worlds.

The business model of the virtual worlds is very different to that of the traditional video-games. Money comes from many different varied sources. In the 1990's, a company would create a gaming console as hardware to support and innovative and creative videogame. Consumers would pay a certain amount of money to buy the *Atari* or *Nintendo 64*, and purchase separately the videogame in a flash disk, CD-ROM or any other video format. This business model has been maintained during the early 2000s, until recently. It evolved with the hyper-connectivity of the new consoles and platforms, introducing subscription options to purchase upgrades and updates of the videogames, wear-ons and *skins* for the game characters and other virtual accessories. But still, paying for a service, and a limited revenue model.

Hyper-connectivity brought another element to the business: data. This asset played a similar role in the gaming industry as in the development of social media (could we call it "traditional" social media, again as opposed to the Metaverse?). Suddenly, the money paid by gamers, or subscribers for the hardware and the videogames, became a secondary source of revenue. The true benefit is in the data. Studying game patters and consumer profiles, crossed marketing interests and other elements of targeted marketing. They allow the companies to know their audience better than they know themselves, and market the videogames in a more attractive way. The famous phrase: "if you are not paying for the product, then you are the product"[6] could also be applicable to the gaming industry, and to the Metaverse. Although gaming may still be resilient to it, considering that there is another source of income that the companies need to tender, the traditional subscriptions and purchases of videogames.

It is still to be seen which way the Metaverse may go, as a business model. We know that the development of the Open Internet in the last 20 years has been towards the profitability of big data analysis and exploitation of personal data. Increased in scale and social impact by the inception of traditional social media, which is even hungrier of data. Without entering the terrain of speculation, it seems safe to say that data plays and will play a very important role in the economic model of the Metaverse.

This big data-driven model is key for the development of the Metaverse. It is key for its technical development, in terms of content creation and interaction with Artificial Intelligence. Only with massive amounts of data, the virtual worlds will be able to operate in a way that resembles reality. Otherwise, it will be another scripted on-screen videogame. Regardless of the nature of the data, content creation is developed with the analysis of massive amounts of information. Interaction of the user with the virtual elements that form the virtual world is an example of this issue. For instance:

1. A virtual driving simulator in the Metaverse could be of potential benefit for society. This virtual driving simulator would need the feed of vast information to simulate

[6] Paraphrasing. Originally attributed to Andrew Lewis: https://x.com/andlewis/status/24380177712?lang=es

the car-driving. Similarly to the data needed to replicate human driving when powering autonomous cars.
2. There will be derivatives to this use, such as the videogame-like experience of driving a car in a virtual Nascar race, in a hyper-realistic way not reachable for many of us in offline life.
3. There could be an upscale social interest in driving a Tesla Model Y, or a Ferrari Testarossa, in the Metaverse, instead of a Toyota Prius or a Seat Ibiza.

All these experiences, with their many differences, are part of the data-driven Metaverse model.

Another example of this big-data driven model is the interaction with AI. Only by processing massive amounts of information, an AI system may be trained to interact with us in the Metaverse. For example, by developing in-site virtual assistant chatbots experiences. Or by powering the avatars that populate the virtual world. Or by impersonating us (willingly in this case) and allowing our avatar to live the virtual life without our direct supervision when we are not inside the platform, logged-off. All these uses may be future developments of AI in the Metaverse that will need a big amount of data.

Data is also paramount for the escalation of the Metaverse in society as a service. Platforms that operate virtual worlds want to understand consumers' behaviour and interest. They need to understand what drives the user to the platform, and what drives him out of it. Currently, most of the interaction of the general public online is in the Open Internet and traditional social media platforms. The Metaverse is an alternative model that will need to analyse users behaviour to thrive as a business model, competing or complementing the aforementioned.

Personal data plays a very important role in this business model development. On the side of technical development, the platform operating the virtual world may need to process personal data to customise the experience for the user. Also to improve the relation between the user and the virtual world interface. Considering the previous examples:

1. A virtual driving simulator in the Metaverse could be of potential benefit for society. This virtual driving simulator may be improved by processing personal data of the user. Either to customise the experience, offering alternative roads or interaction depending on the experience in driving, age or driving tendencies. Or to register the activity for legal implications, such as the validation of a number of hours spent in the simulator as a requisite for certification.
2. In the videogame-like experience of driving a car in a virtual Nascar race, in a hyper-realistic way, personal data may be needed to organise competitions related to our identity between users, or to validate online driving permits and restrict under-aged activity.
3. On the upscale social interest in driving a luxurious car, the need for personal data is even more simple. The platform may need to check your payments to offer you access to a service that you can actually afford. And the users may want to be identified (or identifiable) to brag around.

But again, data, and most importantly personal data play a very important role in the development of the Metaverse in society as a service. Societal scalability of the Metaverse may only be reached with a deep insight into customers interests. Fixation and retention in the platform can only be achieved by offering content and interaction that the user finds attractive. In terms of competition against traditional social media, only by

adopting their means can the metaverse thrive. Twitter-X, Facebook, Instagram, Tik Tok and the rest prey on the personal data of the users to offer them engaging content and obtain revenue through targeted marketing.[7] The Metaverse may need to do the same in the future.

However, the adherence of new users not only depends on the insight on their likes and targeted marketing. Currently, there is a barrier in the Metaverse experience at hardware level. VR glasses are perceived as an uncomfortable device, not suited for long sessions of use. However, there are steep advancements on this side to improve comfort and usability.[8] At medium term, holographics[9], enhanced or mixed reality[10] may be an alternative. But they are not enough technically developed at the moment. It is also a matter of adherence. The users need to perceive the Metaverse as a reliable environment for serious things. As serious as a videogame can get, they do not have enough traction, especially for a more conservative segment of population. This is known as the risk in the gamification[11] dynamics. A certain segment of the population will only be driven to the Metaverse if they see serious and impactful events happening that may affect their lives. It is the reliability of the concept. Corporations managing the virtual worlds should be interested in developing trust for the users to develop work-related activities, payments, artistic activities...

The risks in gamification were highly overcome by the COVID-19 pandemic. Suddenly, companies who were absolutely reluctant to digital activity, were forced to move full-online. Social activities like family gatherings and music concerts, which were only thinkable in the offline world before the pandemic, were forcefully moved to digital platforms. There is no coming back from there.[12] There has been a step forward towards digitalisation and generation of data, which has impacted the development of technologies such as artificial intelligence lately. This step forward will help the inception of the Metaverse as a global digital service, if the key stakeholders are able to hold the momentum.

2. Metaverse and Privacy Laws

We have established the reasons for the importance of the processing of personal data in the Metaverse. It is part of the business model of the data-driven virtual worlds. And it is necessary for its development as a mass service.

It is important to highlight that virtual worlds do not equal the Metaverse. The comparison between the two could be assimilable to the one between the Internet and web

[7] Galloway S, The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google (Conecta Editorial 2017), Chapter 4.

[8] Ray-Ban (Luxottica Group S.p.A.) partnership with Meta, Inc. as an example: https://www.meta.com/es/smart-glasses/

[9] Florian Hechenberger, Kiminad A Mamo and Ismail Zahed, 'Threshold Photoproduction of ${\ensuremath{\eta}}_{c}$ and ${\ensuremath{\eta}}_{b}$ Using Holographic QCD' (2024) 109 Physical Review D 074013.

[10] Raji MA and others, 'Business Strategies in Virtual Reality: A Review of Market Opportunities and Consumer Experience' (2024) 6 International Journal of Management & Entrepreneurship Research 722.

[11] Wanick V and Stallwood J, 'Brand Storytelling, Gamification and Social Media Marketing in the "Metaverse": A Case Study of The Ralph Lauren Winter Escape' in Eirini Bazaki and Vanissa Wanick (eds), Reinventing Fashion Retailing: Digitalising, Gamifying, Entrepreneuring (Springer International Publishing 2023) <https://doi.org/10.1007/978-3-031-11185-3_3> accessed 2 June 2024.

[12] Horgan D and others, 'Digitalisation and COVID-19: The Perfect Storm' (2020) 5 Biomedicine Hub 1.

pages hosts. The Metaverse is global as the Internet is to web pages hosts. Virtual worlds are individual representations of the Metaverse In this paper, however, the two concepts are used interchangeably when the nuance is not necessary. Based on the principle that ¨virtual worlds¨ is the definition adopted by the European Union institutions when developing the concept of the Metaverse.[13]

Virtual worlds are currently run by different corporations, in a granularity comparable to the early days of the Open Internet. Currently, there is no single operator of a unified Metaverse. There is no platform that allows the interoperability between the multiple virtual worlds. But those interested in its scalability (read Meta, Inc.[14], but not only) certainly want to benefit from the free flow of data.

Free flow of data is encouraged almost everywhere in the world. Most of the economies of the OECD are in a race to gain advantage in the sharing of industrial data. It is seen as a global economic benefit that boosts innovation. Even if those data are not shared globally, or even between countries, there is an encouragement to allow the access inside a jurisdiction. Some examples in the European Union:

- The European mobility data space[15] is an example of these initiatives at public level.
- The Data Act[16] and the Data Governance Act[17] are active legislative efforts to build these data pools at European level.
- The European Health Data Space[18] is another example, even if it is not strictly industrial data, but rather personal anonymised information.

The free flow of industrial data already has implications in the development of the Metaverse. For instance, the initiative by Renault Group's industrial Metaverse[19] Renault´s factories have been integrating Virtual worlds into their manufacturing since 2022. T Their goal was to leverage the numerous benefits offered by digital integration in car manufacturing. By expanding their factories into the Metaverse, they aimed to create digital replicas of every factory. This included not just the infrastructure and warehouses, but also every piece of machinery, from the smallest screwdriver to the most advanced robot on the production line. This integration enabled the creation of a digital space where various software systems could interact, allowing for the control of obsolescence even for the oldest hardware. Their development of their own virtual world allowed them to manage

[13] See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition available at https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition

[14] Deslandes N, 'Meta's Vision: How the Metaverse Will Impact Businesses' TechInformed (21 July 2023) <https://techinformed.com/metas-vision-how-the-the-metaverse-will-impact-businesses/> accessed 3 June 2024

[15] https://www.eiturbanmobility.eu/deployemds-open-opportunities-to-create-a-common-european-mobility-data-space/

[16] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, OJ L, 2023/2854, 22.12.2023, (Data Act).

[17] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 OJ L 152, 3.6.2022, p. 1–44, (Data Governance Act).

[18] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

[19] As developed in 2024 https://www.youtube.com/watch?app=desktop&v=I2NtmlahbDU
And announced by their CEO in 2022 https://www.linkedin.com/pulse/renault-group-settles-future-its-industrial-metaverse-renaultgroup-cehie

to overcome some challenges, in a way that no other digital tool could have achieved. Benefitting, thus from the processing of industrial data at a large scale.

It is evident that host companies of virtual worlds target maximisation of their profits. Metaverse stakeholders will certainly be able to benefit from this free-flow of data. But the benefit is not only in the processing of industrial data at a large scale. It is also in the processing of the data of their users. Personal information.

However, when we move to personal data, the story changes. Personal data free-flow is not encouraged everywhere in the world. Take the efforts of the People's Republic of China to keep the data of their citizens inside their territory.[20] Or the very own of the European Union by imposing equal rules of protection of personal data before allowing the flow to third countries.[21] Data localisation plays a very important role in this regard. The control of the personal data of the citizens is regarded by many countries as part of their digital sovereignty, and the protection of their own citizens before predatory companies and geopolitical rivals.

Personal data is protected. All around the world. Privacy has long been considered as a fundamental human right in the offline world.[22] Personal data protection became an important element of the Open Internet. Particularly since the advent of targeted marketing campaigns. As it is also currently an important topic in traditional social media.

Processing of personal data is important in the development of the virtual worlds. Take for instance the examples around automobiles in the previous chapter of this paper. Personal data is also protected in the Metaverse. Rightfully so. Take these few examples:

- When logging into the platforms, it could be required to process certain personal data to prove the age of the user. Minors could be blocked from access, or limited in the content they could access in the virtual world, if they may be exposed to violence or adult content. This processing should be developed in a way that respects privacy, in order to avoid negative impacts to users and deter their use.
- A data subject may want to use their biometric data to identify himself in the Metaverse. For instance, to launch payments securely. These data are extremely profitable and vulnerable to hacking. Security and privacy by design measures may be needed to protect the user.
- Predatory tactics of targeted marketing could be developed in the Metaverse, as well as in the traditional social media industry. Remember those snickers you searched for last week? Or those holidays in Rome you were interested in? Now they are following you also to the Metaverse. These practices may be legitimate to a certain extent, but with stern information impositions and consent developments on the controllers.

Some authors argue the processing of personal data hinders innovation. A point often made by the data-hungry digital industry. Nevertheless, it is not the objective of this paper to debate around this topic. It is enough to acknowledge here the existence of this debate.

The reasoning behind is, in any event, quite plain. The free processing of the personal data in the examples abovementioned would bring potential benefits to the virtual world host that are reduced is the processing is limited:

---

[20] Khasanova L and Tai K, 'An Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localisation Models' (31 July 2023) <https://papers.ssrn.com/abstract=4527052> accessed 3 June 2024.
[21] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[22] Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 193

- Limiting the access of minors to the platforms means that the virtual world reduces its target, losing customers. A flawed mechanism of age control could lead to distrust in the users, who would reduce their time spent in the platform.
- Security and privacy by design measures are often expensive. Encrypting the data and secure storage mean applying procedures that elevate the structural software operational costs.
- Is it truly needed to explain why a company loses money if the targeted marketing is limited? I am probably not going to buy those sneakers if I do not see that advertisement a hundred times on a row.

Data protection could hinder innovation. And it may diminish the profits of the corporations hosting the Metaverse. Therefore, the corporations operating the virtual worlds may want to avoid the application of data protection rules, in order to maximise their profits of processing the personal data. The protection of personal data leads to limitations in the data-driven business model of the Metaverse.

3. Extraterritoriality of privacy laws and the virtual worlds

One clear way to avoid the application of data protection limitations when processing personal data is to develop the operations in jurisdictions where there are no privacy laws. Or at least, lesser protection to privacy. This is quite clear when it is chosen to host digital services in countries with lesser protection, and market the digital services directly there. An example, outside the scope of the Metaverse, but potentially related to it, could be the company Telegram. This instant messaging app is hosted in servers around the world, with a strong presence in the Russian Federation, and other of their allied states.[23] Data protection avoidance is not the main reason behind this corporate decision, but rather the origin of the company and the dodging of intellectual property rights.[24] Telegram is an example of a digital service hosted and primarily offered in a jurisdiction with a lower protection of privacy rights.

However, Telegram has a global reach. That introduces the elements of globalisation and extraterritoriality. Most digital services around the world are hosted in a unique jurisdiction, or a handful of them, and offered worldwide. From a Western perspective, we may provide the example of Youtube (marketed by Alphabet, Inc). An American company (USA based) marketed and offered all around the world. Amongst the target territories, Europe. Where GDPR[25] applies. From an Asian perspective another example may be Tik Tok – Douyin in China. A Chinese company (PRC based), marketed and offered all around the world. Amongst the target territories, Europe. Yet again, where GDPR applies.

Corporations operating the Metaverse may suffer similar pressures, or have a similar background reasoning as the traditional social media companies mentioned before. They may be based and marketed in the same territory, with the same laws applicable. Or

[23] Wijermars M, 'Selling Internet Control: The Framing of the Russian Ban of Messaging App Telegram' (2022) 25 Information, Communication & Society 2190

[24] Isrok M and others, 'Legal Protection of Film Copyright Holders Against the Distribution of Free Film in Telegram Media' KnE Social Sciences 429

[25] 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, OJ L 119, 4.5.2016, p. 1–88 (General Data Protection Regulation).

they may choose a different jurisdiction for the many reasons already explored. Or overcome their origin to be marketed worldwide.

Often, the temptation for the digital behemoths is to process the personal data in a different jurisdiction to the one where the activities are developed. This scenario may present when a company decides to sell its services in a broader market. Or, when already operating in a country, they decide, for any reason, to extract the personal data and move it to a different location.

The reasons to extract the data and process it in a different jurisdiction vary. Some of them could be based on technical development of digital architecture. Data centres are a very important base of the digital industry. Centralisation of the data in selected locations presents advantages in economies of scale. These premises are very complex investments, expensive to build and difficult to maintain. This advantage affects in obvious ways to the development of virtual worlds, which hosting does not vary significatively to other digital architecture.

However, the real reasons tend to be more spurious. Jurisdictions like the European Union protect the personal data imposing measures restrictive to the processing (see examples above). An easy way to circumvent the application of GDPR and other privacy laws (e-Privacy Directive[26] and Law Enforcement Directive[27], for instance) is to develop the processing of personal data outside of this jurisdiction.

EU legislators both in the Data Protection Directive[28] in 1995 and the GDPR in 2016 foresaw this possibility. They introduced the legal institution of the international personal data transfers (Chapter V – GDPR, Chapter V - LED Directive) to limit and avoid the circumvention of privacy laws, as explained in Recital 101 of GDPR:

> *"Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation."*

The ideas defined above are fully applicable to the Metaverse. Scalability of the virtual worlds as a global service may be benefited by the processing of personal data at a large scale. The condition may become *sine qua non* for this development as a high reaching digital service. Innovation, marketing and economies of scale may depend in the virtual worlds on the processing of the personal data in business-friendly jurisdictions.

---

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47 (ePrivacy Directive - Directive on privacy and electronic communications).

[27] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) OJ L 119, 4.5.2016, p. 89–131.

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive – outlawed, no longer in force), OJ L 281, 23.11.1995.

However, the Metaverse presents a significant difference with the previous digital services when facing the extraterritoriality of privacy laws: ubiquity of the personal data. As explained in the next chapter of this paper.

The principle of extraterritoriality of privacy laws inspires the regulation of the international transfers of personal data. GDPR concretely is of applicability for the processing of personal data in other jurisdictions (out of the natural territorial scope of the regulation) under certain circumstances. See article 3 GPDR, for cases like the processing of an undertaking based in the Union, offering of goods or services in the Union, or processing of personal data of residents (not only nationals) of Member States of the EU. When this precept does not apply, rules for transfers in Chapter V of GDPR apply, to avoid the circumvention of the privacy principles. Virtual Worlds are not strangers to these developments, as any other digital service based on the current Open Internet.

A question may arise on where to transfer the data, once the decision of leaving the EU is taken, based on the previously exposed reasons.

The jurisdictions with the lesser data protection limitations are the most attractive. Considering the origin of most of the big-tech companies present globally in the world, China and the United States of America are the go-to options.

Most of the digital companies that market digital services nowadays are based in USA and China[29]. It would be naive to think that it will happen differently with the corporate development of the Metaverse.[30][31]

Transferring the data to China would present certain problems. Not only geo-political issues when large amounts of personal data or sensitive categories, but also directly related to data localisation laws in China. The information about Chinese citizens does not leave the country.[32] For that same reason, the flow of personal data would be very difficult to establish in this jurisdiction.

The Russian Federation represents an interesting example of a stern effort for data localisation. Although *a priori* not so attractive for foreign investment nowadays, it would be appreciable to consider it as an alternative to host digital services globally, with lesser restrictive measures. At least when it comes to digital rights. Russia has implemented several measures, including a legal requirement to store personal data of Russian citizens on servers within the Russian Federation[33] and a ban on VPN services that provide access to blacklisted websites[34]. These actions support the goal of creating a 'sovereign' Russian internet, which can function independently from the global internet in the event of a significant external threat to its integrity. Again, for these reasons, the flow of personal data with other globalised countries would be currently unthinkable.

If the Metaverse were to ever be developed as a universal digital service, it would need to be done after an assessment of these circumstances. In a similar way as the development of traditional social media has faced limitations by jurisdiction. And the most probable destination for the global personal data would be the United States of America.

---

[29] Forbes Top 100 Digital Companies. Available at https://www.forbes.com/top-digital-companies/list/2/#tab:rank

[30] Cheng S, 'Metaverse and Investing' in Shenghui Cheng (ed), Metaverse: Concept, Content and Context (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-24359-2_9> accessed 4 June 2024.

[31] Qin Y, 'Investment Potential Analysis on Chinese Stock Market in Metaverse- Take VR Industry as a Sample' (Atlantis Press 2022) <https://www.atlantis-press.com/proceedings/icfied-22/125971757> accessed 4 June 2024

[32] Ibid [20] Khasanova L and Tai K.

[33] Federal Law No. 242 of 21 July 2014.

[34] Federal Law No. 276 of 29 July 2017.

The USA has been for the last 2 decades a Wild West in terms of digital regulation. With its advantages and disadvantages. It represents now, between the OECD countries (at least one of) the most liberal in terms of the processing of personal data. And the laxest with respect to the right of privacy online. Regardless of the recent efforts in passing a comprehensive federal privacy law[35][36], it continues to be so.

Transferring the data to the USA, is the obvious option for Western based companies operating in the Metaverse. However, as previously exposed, the over-reaching nature of the Metaverse as a digital service may present peculiarities when facing privacy laws, namely the ubiquity of the information.

4. Ubiquity of personal data in the Metaverse

The very nature of the Metaverse as a digital service invites the free-flow of the personal data. It could be argued that this element is also present in the current Open Internet and traditional social media industry. However, there are some features that exacerbate the ubiquity of information in the virtual worlds:

- The virtual worlds are, per nature, overreaching and expansive. The more activity is developed there, the more they need to grow. This affects their global development and reaching worldwide. They need the free flow of data for this reason.
- Users of the virtual worlds want to be everywhere. If concern about data protection was of critical representation in traditional social media, it will be even lesser in the Metaverse. Users (or data subjects) will certainly care less about their privacy and be more willing to its trade-off for free digital services.
- Regulation and legal limits in terms of privacy will be more difficult to apply in the Metaverse than in any other digital platforms. The overreaching nature of the Metaverse forcibly will make enforcement tougher and (even) less realistic than in the current digital *status quo*.

For all these reasons it is solid affirmation to state that information, included personal data will be ubiquitous in the Metaverse, therefore compromising privacy[37] as we know it in the Open Internet.

5. Conclusion

The Metaverse big-data driven model suffers from many similar flaws as the Open Internet and traditional social media do. It is also hungry for data. And more specifically, personal data. However, we are currently in a phase when these flaws or downsides could be overcome by building secure and trust-worthy environments. When it comes to personal

[35] Nahra KJ and Jessani AA, 'New Federal Privacy Bill Draft Hits Congress' (WilmerHale Privacy and Cybersecurity Law, 19 April 2024) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240418-new-federal-privacy-bill-draft-hits-congress> accessed 4 June 2024.

[36] US Senate, 'Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation' (U.S. Senate Committee on Commerce, Science, & Transportation, 7 April 2024) <https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation> accessed 4 June 2024.

[37] Kramcsák, P.T., Papakonstantinou, V., 'Personal Data processing within Immersive Virtual Worlds: Privacy challenges in the interconnected data-driven Metaverse' (2023) MetaverseUA Chair Research Paper #1.

data, the international personal data transfers play an important role in this perception. Building a secure environment where the fundamental right to privacy is respected will bring benefits to society and to the escalation of the Metaverse as a service of masses. How to do so? By spotting the down-pits in the current privacy legislation and overcoming them.

But there are and it needs to be attracted to it, finding it a more secure environment than traditional social media.

People need to trust the digital services in order to use them. So it is also for the Metaverse. The best way to impulse its development is to guarantee privacy and respect for a personal life through it.

Bibliography

Baer RH, *Videogames: In the Beginning* (Rolenta Press 2005).

Brookhaven National Laboratory, 'History:The First Video Game?' https://www.bnl.gov/about/history/firstvideo.php accessed 1 June 2024.

Cheng S, 'Metaverse and Investing' in Shenghui Cheng (ed), Metaverse: Concept, Content and Context (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-24359-2_9> accessed 4 June 2024.

Christensen MA and others, 'Direct Measurements of Smartphone Screen-Time: Relationships with Demographics and Sleep' (2016) 11 PLOS ONE.

Deslandes N, 'Meta's Vision: How the Metaverse Will Impact Businesses' TechInformed (21 July 2023) <https://techinformed.com/metas-vision-how-the-the-metaverse-will-impact-businesses/> accessed 3 June 2024

Galloway S, The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google (Conecta Editorial 2017)

Graetz JM, 'The Origin of Spacewar' [1981] Creative Computing magazine <https://www.wheels.org/spacewar/creative/SpacewarOrigin.html> accessed 1 June 2024.

Hechenberger F, Mamo KA and Zahed I, 'Threshold Photoproduction of ${\ensuremath{\eta}}_{c}$ and ${\ensuremath{\eta}}_{b}$ Using Holographic QCD' (2024) 109 Physical Review D 074013

Horgan D and others, 'Digitalisation and COVID-19: The Perfect Storm' (2020) 5 Biomedicine Hub 1.

Kemp S, 'Digital 2024: Global Overview Report' (DataReportal, 31 January 2024) <https://datareportal.com/reports/digital-2024-global-overview-report> accessed 1 June 2024.

Khasanova L and Tai K, 'An Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localisation Models' (31 July 2023) <https://papers.ssrn.com/abstract=4527052> accessed 3 June 2024.

Kramcsák, P.T., Papakonstantinou, V., 'Personal Data processing within Immersive Virtual Worlds: Privacy challenges in the interconnected data-driven Metaverse' (2023) MetaverseUA Chair Research Paper #1,

Nahra KJ and Jessani AA, 'New Federal Privacy Bill Draft Hits Congress' (WilmerHale Privacy and Cybersecurity Law, 19 April 2024)

<https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240418-new-federal-privacy-bill-draft-hits-congress> accessed 4 June 2024.

Qin Y, 'Investment Potential Analysis on Chinese Stock Market in Metaverse- Take VR Industry as a Sample' (Atlantis Press 2022) <https://www.atlantis-press.com/proceedings/icfied-22/125971757> accessed 4 June 2024.

Raji MA and others, 'Business Strategies in Virtual Reality: A Review of Market Opportunities and Consumer Experience' (2024) 6 International Journal of Management & Entrepreneurship Research 722

US Senate, 'Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation' (U.S. Senate Committee on Commerce, Science, & Transportation, 7 April 2024) <https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation> accessed 4 June 2024.

Wanick V and Stallwood J, 'Brand Storytelling, Gamification and Social Media Marketing in the "Metaverse": A Case Study of The Ralph Lauren Winter Escape' in Eirini Bazaki and Vanissa Wanick (eds), Reinventing Fashion Retailing: Digitalising, Gamifying, Entrepreneuring (Springer International Publishing 2023) <https://doi.org/10.1007/978-3-031-11185-3_3> accessed 2 June 2024.

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 193

Wijermars M, 'Selling Internet Control: The Framing of the Russian Ban of Messaging App Telegram' (2022) 25 Information, Communication & Society 2190.

MetaverseUA
Chair

Universitat d'Alacant
Universidad de Alicante