ITUPublications

International Telecommunication Union

Standardization Sector

ITU Focus Group Technical Report

(12/2023)

ITU Focus Group on metaverse

Regulatory and economic aspects of the metaverse: Data protection

Working Group 7: Economic, regulatory & competition aspects

Technical Report ITU FGMV-14

Regulatory and economic aspects of the metaverse: Data protection

Summary

In a world still striving to secure data protection and data sovereignty, the metaverse is one of the latest trends in technological developments and waves, and one which involves a wide range of economic activities in a non-regulated new world. Similar to its previous counterparts, the idea opens up a multitude of risks and threats, which go hand in hand with the opportunities it creates. This Technical Report (TR) tries to explore the possible data protection concerns in the metaverse, in terms of regulatory and economic perspectives. This TR is divided into two parts: general data protection-related concerns and economic data protection-related concerns. The data protection topic is considered a foundational base for conducting economic activities in the metaverse and for regulating all activities of the metaverse. This contribution approaches this novel topic through the 'Life Cycle of Data Threat Model' that tries to pinpoint some threats at different stages of the data lifecycle. The model depends on dividing the lifecycle of data into seven stages: data generation, data transfer, data usage, data sharing, data storage, data archiving and data destruction. This contribution finally presents a data protection assessment framework that can be used to assess the level of threat of each of the challenges presented, and therefore policy priorities may be determined accordingly.

Keywords

Avatars, data lifecycle, data privacy, data protection, data sovereignty, economic activity, metaverse, national security, security threats.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1.0 of the ITU Technical Report on "Regulatory and Economic Aspects in the metaverse: Data Protection-Related" approved at the 4th meeting of the ITU Focus Group on metaverse (ITU FG-MV), held on 4-7 December 2023 in Geneva, Switzerland.

Acknowledgments

This Technical Report was researched and written by Ahmed Said (Ministry of Communications and Information Technology, Egypt) and Hedaia Nabil (Ministry of Communications and Information Technology, Egypt) as a contribution to the ITU Focus Group on Metaverse (FG-MV). The development of this document was coordinated by Andrey Perez (Anatel, Brazil) and Okan Geray (Digital Dubai, United Arab Emirates), as FG-MV Working Group 7 Co-Chairs.

Additional information and materials relating to this report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact Cristina Bueti at tsbfgmv@itu.int.

Editor:	Ahmed Said Ministry of Communications and Information Technology Egypt	Tel: +20 1002527334 E-mail: ahmed.said@mcit.gov.eg
Editor:	Hedaia Nabil Ministry of Communications and Information Technology Egypt	Tel: +20 1222388796 E-mail: hedaia@mcit.gov.eg
WG7 Co-Chair:	Andrey Perez Anatel Brazil	E-mail: andreyperez@anatel.gov.br
WG7 Co-Chair:	Okan Geray Digital Dubai United Arab Emirates	E-mail: Okan.Geray@digitaldubai.ae

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Technical Report	1
4	Abbreviations and acronyms	1
5	Conventions	1
6	Introduction	1
7	Data protection and privacy concerns in the metaverse	2
7.1	Complicated roles	2
7.2	Data sharing and portability	2
7.3	Increase in the sources of data collection	3
7.4	Mass profiling	3
7.5	Proliferation of illegal and harmful content	4
7.6	The legal identity of avatars	4
7.7	Intellectual property rights protection	4
7.8	Sharing data for investigative purposes	4
7.9	Digital sovereignty implications	4
8	Economic-related data protection concerns in the metaverse	4
8.1	Concerns related to trademarks and trade secrets in the metaverse	5
8.2	The overlap and ambiguity in relation to virtual goods and their real counterparts	6
9	Data protection threat assessment framework	6
10	Conclusion	8
Bibliography		9

Technical Report ITU FGMV-14

Regulatory and economic aspects in the metaverse: Data protection-related

1 Scope

The scope of this Technical Report is confined to approaching the regulatory and economic aspects of the metaverse from a data-related perspective, with the aim of putting more focus and depth of analysis in a specific area of the wide regulatory and economic concerns of the metaverse, specifically data protection concerns. So, this Technical Report tries to touch as much data-related concerns as possible in general and in the economic realm inside the metaverse. This is differentiated from the scope of the work of WG6 in the sense that the contribution focuses on data-related issues from the regulatory perspective, rather than from the technical perspective of securing data.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AR	Augmented Reality
DAOs	Decentralized Autonomous Organizations
GDPR	General Data Protection Regulation
NFT	Non-Fungible Token

5 Conventions

None.

6 Introduction

The metaverse has been lately gaining noticeable attention. The term 'metaverse' first originated in two novels: Neal Stephenson's 1992 'Snow Crash' and Ernest Cline's 'Ready Player One'. These versions of the metaverse matter because they proved to be self-fulfilling. Both versions present the metaverse as 'a massive, persistent, open and economically developed virtual world', in the sense that it is a world that never pauses, open for anyone with VR hardware, where avatars can work, socialize, play and carry out extensive trading of goods and services through electronic currencies [b-Gilbert, S.].

The metaverse depends on several essential technologies: virtual reality (VR) and augmented reality (AR) that facilitate the entrance to the three-dimensional online environment through dedicated headsets and other devices connected to computers or games consoles. Artificial intelligence helps

create a virtual version of each user, called an 'avatar', who is the main player inside the metaverse, and is also used for seamless communications along with Internet of Things technology. Economic underpinnings of the metaverse include cryptocurrencies and non-fungible tokens (NFTs) to monetize transactions inside the online world, backed by blockchain technology which helps in providing trust in the economic transactions.

The metaverse is expected to present huge economic and social opportunities such as in the health, education and industry sectors. However, this comes with a high cost; there is a wide range of risks on privacy, data protection, identity, cybersecurity, ownership, misuse and digital sovereignty, as well as economic and social risks such as the impact on vulnerable groups. Despite still being quite far from the proposed model with its prerequisites, the world is witnessing steady developments and manifestations of applying the idea but it is still quite scattered though, featuring separate small metaverses rather than a one global metaverse.

In this preparatory scene, it is very important to study the regulatory aspects of the metaverse and possible implications on privacy and data protection are one of the biggest challenges posed by the metaverse. This Technical Report is divided into two parts; the first sheds light on privacy and data protection concerns in the metaverse and how countries are preparing themselves for these challenges. In this part, the Technical Report uses the 'Life Cycle of Data Threat Model' [b-D., Mai Mansour] in order to analyse the threats presented by the metaverse according to the lifecycle of data. The model depends on dividing the lifecycle of data into seven stages: data generation, data transfer, data usage, data sharing, data storage, data archiving and data destruction. The second part tackles economic-related data protection concerns in the metaverse. This Technical Report finally presents a data protection assessment framework that can be used to assess the level of threat of each of the challenges presented, and therefore policy priorities may be determined accordingly.

7 Data protection and privacy concerns in the metaverse

As portrayed above, the metaverse will bring new dimensions to the data protection and privacy scene. Where regulations of data protection have been so far tackling physical data about users/ people, and its movement between countries, the metaverse world will create totally new actors (avatars) in addition to the original users with large amounts of data generated from new sources such as the data collected from facial and eye expressions, moving between different metaverses. This general idea carries many complications, concerns and policy issues to consider in terms of privacy and data protection. Some of the data protection and privacy concerns in the metaverse are presented in this clause.

7.1 Complicated roles

The metaverse world blurs the roles and responsibilities that have been established by data protection regulations throughout the past years. It is difficult to determine responsibilities and liabilities in the metaverse. This is even more dangerous in light of the large amounts of data generated in the metaverse. It is unclear now who is responsible for storing, processing and safeguarding data. Also, it is unclear who is responsible for compliance with laws and regulations where it was normally the controller's responsibility to ensure individuals can exercise their rights and parties comply with laws and regulations. Data agreements may also be very challenging in a decentralized world. [b-European Parliament], [b-Smith, R.].

7.2 Data sharing and portability

The metaverse will connect the person to their "avatar" or other digital representations. Therefore, countries would likely consider information collected about a metaverse user's activities to be personal data, subject to existing privacy and data protection laws. This raises complicated issues such as jurisdictional responsibilities, as well as portability and interoperability considerations. [b-Smith, R.].

The metaverse presents problems of interoperability and movement of users inside and between different metaverses, together with their data and assets. This creates duplication with the real-world movement of data. Determining jurisdictions in the metaverse is very challenging as a result of adding a new important player "the avatar". Will jurisdiction apply according to the location of the real-world user or the avatar? Some additional contractual requirements apply in many countries in addition to some localization requirements, it is unclear how will this be handled in the metaverse. It is also unclear how concepts of 'extra-territorial reach' present in the GDPR and other regulations will be applied in the metaverse. The duplication created in data production as a result of the new actor's presence shall be regulated. [b-European Parliament], [b-Abd Al Ghaffar, Hedaia-t-N], [b-Martin, B.].

7.3 Increase in the sources of data collection

Users are likely to be providing more information about themselves than they are doing today as a result of the diversity of sources of data collection. Instead of dealing with clear sources of data collection in the current situation, the metaverse will introduce new sources of data collection that may be very challenging to get users' consent on, such as eye trackers that could give data and insights about emotions through the interpretation of facial expressions and brain wave patterns. Some legal experts recommend that metaverse regulations should be designed to limit the scope of emotion-responsive advertising.

Additionally, the modes used in the metaverse can pose high risks that can be used to infringe privacy. In the metaverse environment, players move their avatars around and the scene is observed by the player who can take either a first-person perspective and look through the eyes of their avatars, or a third-person perspective where the camera is not attached to the avatar allowing the player to watch both their own avatar and the environment around them. In the third-person perspective, which is sometimes the default, the camera can move independently of the avatar and can be taken to locations different from the avatars'. This practically allows the player to use the camera as a spying device. Furthermore, the camera can be attached to another avatar without this avatar's awareness. [b-European Parliament], [b-Leenes, R.].

One example of data sources that infringe privacy in the metaverse is some devices used in games such as Second Life Game. [b-Second Life] A wristwatch for example, is provided for free in the Second Life. The watch reports the location of the watch wearer, plus any other avatars in proximity, then this data is reported to a database outside the virtual realm. The behaviour of the watch wearer's friends within the avatar's proximity is monitored. Friends are unaware of the watch's function. Since the database is hosted on a website outside the virtual realm, it is within reach of real-world search engines. This kind of real-virtual interaction poses privacy concerns and possible data protection infringements. [b-Lee C., et.al.], [b-Leenes, R.].

7.4 Mass profiling

With reference to the above concerns, the metaverse poses risks of mass profiling that can be used for advertising, controlling people's decisions socially, politically and economically, as well as posing risks about more state surveillance, through access to sensitive data such as emotional reactions and biometric data. The metaverse is expected to exacerbate the current situation of data collection about citizens and mass profiling, due to the wider sources of data collection which helps governments collect data not only about people's personal information and behaviour but also about the internal reactions of people towards different things seen or experienced and relate accordingly to how they react. This would allow a highly accurate prediction of behaviour and consequently allow for clearer mass profiling and easier manipulation of people. This may directly pose risks to the national security of countries. [b-Abd Al Ghaffar, Hedaia-t.N. (1)].

7.5 Proliferation of illegal and harmful content

The metaverse is described as one of the decentralized autonomous organizations (DAOs), where avatars are the main content creators. It is unclear how the metaverse can regulate illegal and harmful content such as sexual harassment, disinformation, extremist ideas and pornographic content.

7.6 The legal identity of avatars

It is still unclear whether it is necessary to grant legal personality to avatars to hold them responsible for their actions. Will this be separate from the legal identity of the original users or are they linked? Does this pose risks to data protection and the risks of user identification? Since there are no specific laws regulating avatars, the content that users reveal via avatars may breach the personal protection of users and make them identifiable. Additionally, it is allowable in the metaverse to create alternate accounts, named as Alts, which allows users to engage in the metaverse with different identities. These Alts provide a kind of anonymity which can be used for illegal acts and behaviours. [b-European Parliament], [b-Smith, R.], [b-Leenes, R.].

7.7 Intellectual property rights protection

It is challenging to guarantee intellectual property rights in the metaverse, where content is distributed and replicated through Web 3.0 and blockchain-based platforms. NFTs were presented as a technical solution; however, this may raise issues around the applicable law and jurisdictions. [b-European Parliament], [b-Smith, R.] There are several types of intellectual property in the metaverse: copyright protection of virtual objects such as avatars and objects, trademark protection of logos and brands, and patent protection in relation to technological advancements in the metaverse. In the metaverse, users can create virtual representations of real-world objects, which may include copyrighted work or trademarks they do not own. It is also controversial whether the avatars would be subject to copyright protection in case a person created an avatar of a real existing person.

7.8 Sharing data for investigative purposes

It is still vague how the data in the metaverse will be shared for investigative purposes. Cross-border investigations involving the metaverse must be safeguarded by international treaties balancing considerations of security and data protection and privacy.

7.9 Digital sovereignty implications

The metaverse poses extensive risks regarding the digital sovereignty of countries: how countries will be exercising sovereignty of their land and citizens in all meanings; will the avatars be citizens; and how would the sovereignty over land be exercised in the metaverse. The scene has also witnessed many governments introducing digital banks in the metaverse; how will they exercise sovereignty versus the real world and how will they exercise sovereignty over their economies and currencies in the metaverse?

Some national values may be at risk as well, such as how freedom of expression and the protection of human rights and dignity may be guaranteed. Shall the metaverse get the world history back to some practices that the world bypassed throughout the years through regulations? The answers are still unclear; however, some strong endeavours have been made regarding how the principles of the Human Declaration of Human Rights can be applied to the metaverse. [b-CMS], [b-ITU-T FGMV-06].

8 Economic-related data protection concerns in the metaverse

In addition to the above concerns related to data protection, carrying out economic activities in the metaverse poses extra regulatory concerns and risks, such as those in the following subclauses.

8.1 Concerns related to trademarks and trade secrets in the metaverse

Doing businesses in the metaverse raise concerns related to trademark assessment and ways for classification of trademarks for metaverse activity and digital assets, as well as ways of avoiding trademark infringement and business identity theft, in addition to the threats related to disinformation about transactions and financial matters. This is especially important in light of the absence of legal concepts of habitual residence, domicile place of business, which are traditionally at the core of national and international laws and rules that protect data rights and regulate identity thefts, and in light of the clear increase in the number of trademark applications for virtual goods and services. According to a report from May 2022, the increase in popularity of the metaverse and NFTs raised Class 9 of the Nice Classification (including computer hardware and software) to second place by the end of 2021.

Some intellectual property concerns are very clear in trade in the metaverse due to the infringements threat, such as the sale of fake artwork under the guise of copyrighted work, patent infringement in production of the hardware associated with the metaverse or misappropriation of trade secrets.

The metaverse involves the handling of massive amounts of user-generated data. Ensuring the security of this data, especially when it pertains to proprietary algorithms or processes, is a significant challenge in intellectual property and trade secret protection. Recent developments in artificial intelligence (AI), along with advancements like machine/sensor-generated data, combined with the present and future computing power for processing datasets and their utilization in innovative business models, have sparked general discussions on the rights associated with data, including intellectual property (IP) rights and trade secrets but not yet with a focus on the metaverse.

In recent years, the issue of rights over data has gained significant traction. Among the various types of IP and IP-like mechanisms, the legal safeguard offered by trade secrets under the EU Trade Secret Directive 2016/943 (TSD) holds promise. Trade secrets encompass any information that is confidential, possesses commercial value due to its confidentiality and has been subjected to reasonable measures to maintain its secrecy. This framework emerges as a viable tool for safeguarding and leveraging substantial amounts of shared data deemed strategically significant.

Exploring beyond the EU, attention should be drawn to Japan. In 2018, Japan amended its Unfair Competition Prevention Act (Act No 47 of 1993) to introduce specific protection for "shared data with limited access." This addresses situations where trade secrets protection may not be applicable to machine-generated data due to challenges in meeting the definition of a "trade secret." Although detailed guidelines exist for interpreting this new regulation, a comprehensive body of legal precedents is yet to evolve. It is worth mentioning that the Japanese cabinet submitted another amendment to the Unfair Competition Prevention Act in March 2023 concerning trade secrets and shared data with limited access. The key changes introduced include strengthening IP protections of businesses in the digital space by expanding types of registerable trademarks and copyrights and strengthening protections against data breaches and infringement in the digital space, as well as supporting international business development by imposing stricter penalties and clarifying procedures for international trade secret infringement cases.

The evolving landscape of the metaverse underscores the critical importance of robust data security measures in the realm of intellectual property and trade secret protection. As the metaverse thrives on vast amounts of user-generated data, proprietary algorithms and collaborative innovations, ensuring the confidentiality, integrity and degree of access to this information becomes key. The dynamic nature of shared environments and decentralized structures within the metaverse necessitates a proactive and adaptive approach to safeguarding intellectual property and trade secrets.

8.2 The overlap and ambiguity in relation to virtual goods and their real counterparts

The complicated relationship between virtual and real goods is an issue of concern that would drive a regulatory action to settle. This vague relationship complicates data and identity protection in the metaverse.

For example, one of the main questions raised is whether the pre-existing registrations for physical goods are sufficient, or if it is necessary to apply separately for trademark rights for virtual counterparts.

In some cases, virtual goods or services are not simply counterparts to physical world goods or services but do relate to them. For example, based on recent trademark applications, McDonald's is planning to operate virtual cafes that offer the ability to order physical-world food to be delivered to the person physically. In other cases, virtual and physical services may be the same. For example, training services can be provided in both the physical and virtual world. However, even in this case, concerns about trademarks arise; whether there is a need for two trademarks or not and where to file them.

Wrap up:

With respect to data protection challenges, and in light of the lifecycle of the data threat model, it can be concluded that the metaverse presents security threats with regard to almost all stages of the data lifecycle. There are many challenges related to the data generation stage (pervasive data collection), such as the increase in the sources of data collection and the legal identity of avatars. Some other challenges are related to data transfer (privacy leakage in data transmission) such as the issues of interoperability of the two worlds and how the data would be transferred. Other challenges relate to the usage stage, such as mass profiling threats and the proliferation of illegal and harmful content. There are also challenges related to the data sharing stage (privacy leakage in data processing) such as the questions posed about the legality of sharing data between the two worlds, as well as the sharing of data for investigative purposes. The same goes for data storage (privacy leakage in cloud/edge storage), archiving and destruction (threats to digital footprint), where the metaverse concept poses many questions about these stages, especially in light of the duplication created between the avatar and the original user which duplicates the amount of threat existing nowadays in this regard. [b-Abd Al Ghaffar, Hedaia-t- N. (3)], [b-Wang, yuntao, et.al.].

9 Data protection threat assessment framework

The metaverse shall be assessed and evaluated before a country may tap into this realm. This section presents a data protection threat assessment framework, based on the ENISA and LINDDUN privacy and threat assessment frameworks [b-ENISA], [b-Maria Grazia Porcedda]. The framework is based on a number of data protection goals that shall be secured in any implemented policy. Assessing each threat against the data protection goals can serve several purposes as it can identify the level of danger each threat poses, whether it is *normal, high, very high* (according to the number of protection goals that the threat infringes) and therefore assess the metaverse as a public policy in regard to its threat to data protection. This assessment can also give an indication to the strength of the national data protection regulation and the areas of weaknesses in it. The assessment can also serve as a guide to the technical solutions and strategies that shall be adopted or implemented and tested ahead of applying metaverse projects.

The assessment framework builds on ENISA's main security and privacy protection goals: [b-ENISA]:

1 *'Unlinkability'*

2 *Integrity*

3 *Confidentiality*

4 *Availability*

5 *Transparency*

6 *Intervenability*

Both ENISA and LINDDUN have introduced operationalization to these goals, to make them clear, dismantled and easy to assess, as follows: [b-Maria Grazia Porcedda].

'Unlinkability': hiding the link between two or more actions, identities and pieces of information:

a) Anonymity: hiding the link between an identity and an action or a piece of information. Pseudonymity: to build a reputation on a pseudonym and the possibility to use multiple pseudonyms for different purposes.

b) Undetectability and unobservability: hiding the user's activities (e.g., impossibility of knowing whether an entry in a database corresponds to a real person).

Integrity: to ensure that processing operations (data, systems, processes) remain:

a) intact

b) complete

c) accountable

d) up to date.

Confidentiality: the protection of communications or stored data against interception and reading by unauthorized persons:

a) hiding the data content or controlled release of data content (e.g., encrypted email).

Availability:

a) the confirmation that data which has been sent, received or stored is complete and unchanged;

b) to ensure that processing operations (data, systems, processes) are available in a timely manner; and,

c) in accordance with national regulations.

Transparency: to ensure that processing operations (data, systems, processes) can be understood, reconstructed and evaluated with reasonable effort.

a) The information has to be available before, during and after the processing takes place. Mechanisms for achieving or supporting transparency comprise logging and reporting.

b) Content awareness: users are aware of their personal data and that only the minimum necessary information should be sought and used for the performance of the function to which it relates.

c) Policy and consent compliance: the whole system, including data flows, data stores and processes, has to inform the data subject about the system's privacy policy or allow the data subject to specify consent in compliance with legislation, before users access the system.

Intervenability: intervention is possible concerning all ongoing or planned privacy-relevant data processing, in particular by those persons whose data is processed. The objective is the application of corrective measures and counterbalances where necessary. Mechanisms for intervenability comprise established processes for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions to prevent lock-in at a data processor, among others:

a) to ensure that processing operations (data, systems, processes) are designed so that the data subjects can exercise the rights granted to them pursuant to the regulation;

b) to ensure that controllers and data protection authorities can intervene in the data processing.

10 Conclusion

The metaverse concept poses many risks and threats to the data sovereignty of countries as a whole. Carrying out economic activities in the metaverse faces all the above-mentioned data protection concerns in addition to others related to trademarks. Countries shall therefore act proactively before the actual introduction of the metaverse as portrayed to minimize the risks posed by the metaverse while getting the good of it. One way this can be done is by assessing the level of threats the metaverse poses. This can help countries in evaluating the strength of their current data protection regulations and their ability to face the possible threats presented by the metaverse. This can also help in setting priorities of the different threats and developing the required defence mechanisms ahead of adopting metaverse projects.

Bibliography

[b-ITU-T FGMV-06] ITU-T Focus Group Technical Report (2023), *Guidelines for consideration of ethical issues in standards that build confidence and security in the metaverse.* Working Group 6: Security, Data & Personally Identifiable Information (PII) Protection. http://handle.itu.int/11.1002/pub/822f50e6-en

[b-Abd Al Ghaffar, Hedaia-t.N. (1)] Abd Al Ghaffar, Hedaia-t.N. (2020), *Government Cloud Computing and National Security*. Review of Economics and Political Science, Vol. ahead-of-print No. ahead-of-print. Available [viewed 2023-11-21] at: https://doi.org/10.1108/REPS09-2019-0125

[b-Abd Al Ghaffar, Hedaia-t.N. (2)] Abd Al Ghaffar, Hedaia-t-Allah Nabil (2021), *Data Protection Laws Trends: Practice and Debate*. Social Science Research, Global Journals. Available [viewed 2023-11-21] at: https://socialscienceresearch.org/index.php/GJHSS/article/view/3882

[b-Abd Al Ghaffar, Hedaia-t.N. (3)] Abd Al Ghaffar, Hedaia-t-Allah Nabil (2023), *Data Protection in the metaverse: Concerns and Implications*. Social Science Research, Global Journals. Available [viewed 2023-11-21] at: https://globaljournals.org/GJHSS_Volume23/2-Data-Protection.pdf

[b-CMS] CMS (2022), *Data Protection Challenges, the importance of cybersecurity, advertising regulation in the metaverse*. Available [viewed 2023-11-21] at: https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-3-data-protection-challenges-the-importance-of-cybersecurity-advertising-regulation-in-the-metaverse

[b-D., Mai Mansour] D., Mai Mansour (2013), *Data Security in Cloud Storage Services*. Master Thesis, American University in Cairo. Available [viewed 2023-11-21] at: https://fount.aucegypt.edu/etds/1201/

[b-ENISA] ENISA (2015) *Privacy and Data Protection by Design*. Available [viewed 2023-11-21] at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[b-European Parliament] European Parliament, European Parliamentary Research Services (2022), *Metaverse: Opportunities, Risks and Policy Implications*. Available [viewed 2023-11-21] at: https://epthinktank.eu/2022/06/24/metaverse-opportunities-risks-and-policy-implications/

[b-Gilbert, S.] Gilbert, S. (2022), *The Political Economy of the Metaverse*. Instituit Francais Des Relations (Geopolitics of Technology Program). Available [viewed 2023-11-21] at: https://www.ifri.org/en/publications/briefings-de-lifri/ political-economy-metaverse

[b-Lee C., et.al.] Lee C., et.al. (2007), *Security Issues within Virtual Worlds such as Second Life*. Edith Cowan University, Australian Information Security Management Conference. Available [viewed 2023-11-21] at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&conte xt=ism

[b-Leenes, R.] Leenes, R., *Privacy in the Metaverse: Regulating a Complex Social Construct in a Virtual World*. Tilburg University, Netherlands. Available [viewed 2023-11-21] at: https://dl.ifip. org/db/conf/ifip9-6/fidis2007/Leenes07.pdf

[b-Maria Grazia Porcedda] Maria Grazia Porcedda (2018), *'Privacy by Design' in EU Law*. Matching Privacy Protection Goals with the Essence of the Rights to Private life and Data Protection, in M. Medina, N. Tsouroulas, K. Rannenberg, E. Schweighofer and A. Mitrakas, Annual Privacy Forum 2018, Lecture Notes in Computer Science, Springer-Verlag (forthcoming). Available [viewed 2023-11-21] at: https://eprints.whiterose.ac.uk/134061/1/Porcedda_Privacy_by_design.pdf

[b-Martin, B.] Martin, B. (2022), *Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse*. Harvard Journal of Law and Technology, Volume 36, Number 1. https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf

[b-Second Life] *Second Life Game*. Available [viewed 2023-11-21] at: https://secondlife.com/

[b-Smith, R.] Smith, R. (2021), *Reed Smith Guide to the Metaverse*, Issue 1. Available [viewed 2023-11-21] at: https://www.reedsmith.com/en/perspectives/metaverse

[b-Wang, yuntao, et.al.] Wang, yuntao & Su, Zhou & Zhang, et.al. (2022), *A Survey on Metaverse: Fundamentals, Security, and Privacy*. Available [viewed 2023-11-21] at: https://www.researchgate.net/publication/359052509_A_Survey_on_Metaverse_Fundamentals_Security_and_Privacy