Master's thesis 2023
Master of Laws
30 higher education credits

Lost in the Metaverse

Navigating privacy challenges in the jurisdiction of virtual worlds

Adeline Fredriksson

Supervised by Joachim Åhman

Department of Law
School of Business, Economics and Law
University of Gothenburg
Gothenburg, Sweden 2023

"If you're not paying for the product, then you are the product."[1]

[1] Tristan Harris, Google's former design ethicist and co-founder of the Center for Humane Technology, in *The Social Dilemma* (Netflix, 2020), Orlowski, Jeff (dir.).

Abstract

The Metaverse consists of a set of emerging technologies that could be as disruptive as the internet, enabling seamless integration of our digital and physical lives. While offering a wide array of exciting application areas, the technologies also allow for intrusions on our privacy at a higher level than has ever been possible. The data collection, analysis, and processing facilitated by Metaverse technologies could be leveraged to manipulate individuals at far deeper levels than currently possible, challenging the privacy rights granted to individuals under the ECHR.

Against this background, this thesis examines how the technologies of the Metaverse could affect the conceptualization of the right to privacy. The analysis revealed that Metaverse technologies create several privacy concerns, particularly regarding psychological integrity, biometric data collection, and surveillance of physical spaces. These observations highlight the need to adapt the notion of privacy to account for the unprecedented possibilities of virtual privacy violations facilitated by Metaverse technologies.

Additionally, Metaverse technologies enhance the opportunities for virtual human rights infringements, which risks leading to a complex jurisdictional situation. Thus, this thesis investigates the applicability of the ECHR jurisdiction criteria to virtual human rights violations occurring beyond a state's territorial borders. Current models for defining jurisdiction are inadequate for such virtual human rights violations. Physical borders are no longer barriers to committing human rights violations when technology allows states to control the rights of individuals remotely. There is a need to revise jurisdictional models to account for the complexities of human rights in a digital context. Thus, the thesis proceeds to address alternative models for defining jurisdiction, though they are still subject to criticism. Therefore, there is a need for further research on whether jurisdiction remains an appropriate threshold for safeguarding human rights in a digitalized society.

In conclusion, this thesis sheds light on the need for an adapted notion of privacy to effectively address the challenges of Metaverse technologies. Additionally, the thesis highlights the need to reexamine traditional jurisdiction models in the context of virtual human rights violations.

Keywords: Metaverse, human rights, privacy, jurisdiction

Preface

Denna uppsats markerar slutet på mina år på juristprogrammet och universitetet. På många sätt lämnar jag som en annan person än jag var när jag kom hit. Jag kommer alltid att vara tacksam för den utveckling som dessa år har gett mig – professionellt och kunskapsmässigt, men framför allt på ett personligt plan. Det finns många människor som jag vill tacka, men några förtjänar ett särskilt omnämnande.

Tack till min handledare Joachim Åhman för intressanta diskussioner, vägledning och feedback.

De sista två åren på min utbildning har spenderats på mastersprogrammet Intellectual Capital Management på Chalmers Tekniska Högskola och jag vill rikta ett stort tack till hela fakulteten. Särskilt tack till Ulf Petrusson, Christoffer Hermansson, Anna Holmberg Borkmann och Bowman Heiden - ni har visat ett engagemang för vår utbildning som är helt oöverträffat, och jag kommer alltid att ta med mig perspektiven, insikterna och inspirationen ni har gett mig. Även stort tack till min ICM-klass för att ni gjort dessa år lärorika, minnesvärda och otroligt roliga – det har varit ett nöje att få avsluta min universitetstid med er!

Tack mamma, för att du har stöttat mig från början till slut, i toppar och dalar, och alltid räddat mig när jag tagit slut på studielånet för snabbt.

Slutligen tack Petter, för att du tror på mig som ingen annan.

Maj, 2023
Adeline Fredriksson

Abbreviations

Below is the list of abbreviations that have been used throughout this thesis listed in alphabetical order:

AI	Artificial Intelligence
AR	Augmented Reality
DAO	Decentralized Autonomous Organization
ECHR *or* the Convention	European Convention on Human Rights
ECtHR *or* the Court	European Court of Human Rights
EEG	Electroencephalogram
EMG	Electromyography
GDPR	General Data Protection Regulation
ICCPR *or* the Covenant	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
IoT	Internet of Things
NFT	Non-Fungible Token
NPC	Non-Player Character
PoW	Proof of Work
PoS	Proof of Stake
UDHR	Universal Declaration of Human Rights
VR	Virtual Reality
VCLT	Vienna Convention on the Law of Treaties
XR	Extended Reality

Contents

1 Introduction

In this chapter, the overarching topic of this thesis is introduced. This includes an outline of the background and the problem statement addressed in this thesis. Further, the research questions are introduced, along with the methodological framework used to answer them. Lastly, previous research in this area, along with the overarching disposition of the thesis, is summarized.

1.1 Terminology

The terms *virtual human rights violations* and *virtual privacy violations* are continuously used to describe situations where the violation of human rights in general, or the right to privacy specifically, are carried out remotely and by technical means.

The term *Metaverse* refers to a synthesized three-dimensional virtual world made up of user-controlled avatars, digital items, virtual environments, and other computer-generated elements, where people can use their virtual identity through any smart device to communicate, collaborate, and socialize. The term is also used as an umbrella term to describe a set of novel technologies, including AI, blockchain, and XR, that facilitate the development of the Metaverse.

1.2 Background

In the current online world, it is commonly recognized that if you are not paying for a product or service with money, you - or your data - are the product. The widespread use of digital platforms has led to an exponential growth in data collection, storage, and analysis by Big Tech firms and governments.[2] Data is now being treated as a form of property, which is manufactured, transferred, licensed, sold, and stolen.[3] The business model used by these firms relies on sharing personal data between

[2] Constantiou, Ioanna D and Kallinikos, Jannis. 'New games, new rules: big data and the changing context of strategy'. *Journal of Information Technology.* Vol. 30, No. 1. 2015, 44-57.

[3] Ritter, Jeffrey and Mayer, Anna. 'Regulating data as property: a new construct for moving forward'. *Duke L. & Tech. Rev.* Vol. 16. 2017, 220.

users, platforms, and businesses to target advertisements to users. This practice, often called surveillance capitalism, has long raised concerns about privacy rights and the exploitation of personal data.[4] The Cambridge Analytica scandal and the data leakage by Edward Snowden are examples of how data exploitation can threaten human rights.[5]

Currently, we are witnessing the advent of several technologies that have the potential to take surveillance capitalism to new heights. One of these is AI, which is becoming increasingly ubiquitous in our daily lives. Chat GPT is the most current example that marks the beginning of AI becoming a part of our everyday activities. AI technologies are constantly advancing and reaching unprecedented levels of sophistication, with exponential growth expected shortly. In addition, the emergence of wearable technologies, such as VR headsets and AR glasses, is being integrated into various aspects of our lives, from work to entertainment. These wearables can track users' physical movements, emotional states, and reactions in real-time.[6] Furthermore, IoT technologies connect everyday objects to the internet, enabling them to communicate and exchange information with each other and people. This means that objects in our private sphere – take something as trivial as vacuum cleaners - are becoming part of the IoT ecosystem. The public sphere is also affected, with objects like trash cans becoming connected to the internet. These emerging technologies allow for an unprecedented scale of data collection and analysis.

---

4 Zuboff, Shoshana. 'Big Other: surveillance capitalism and the prospects of an information civilization'. *Journal of Information Technology.* Vol. 30, No. 1. 2015, 75-89.

5 Rosenberg, Matthew, Confessore, Nicholas, and Cadwalladr, Carole, 'How Trump Consultants Exploited the Facebook Data of Millions', *The New York Times*, 2018.

6 Ivanova, Ekaterina and Borzunov, Georgii. 'Optimization of machine learning algorithm of emotion recognition in terms of human facial expressions'. *Procedia Computer Science.* Vol. 169. 2020, 244-48; Van Den Broek, Egon L et al. 'Affective man-machine interface: Unveiling human emotions through biosignals'. *Biomedical Engineering Systems and Technologies: International Joint Conference (BIOSTEC 2009).* 2010, 21-47.

These technologies all come together developing Metaverse. The term has gained immense popularity as one of the most talked-about technological phenomenon. It is seen as the next internet iteration that seamlessly integrates our digital and physical lives. In his novel *Snow Crash* in 1992, Neal Stephenson first used the term, which referred to virtual reality worlds where people could design, build, and own virtual assets while interacting with other users.[7] While there is no single, unanimous definition of the Metaverse, it can be summarized as a synthesized three-dimensional world made up of user-controlled avatars, digital items, virtual environments, and other computer-generated elements, where people can use their virtual identity through any smart device to communicate and socialize.[8]

The interest in the Metaverse has grown exponentially in recent years. Facebook changing their name to Meta and announcing that the social media giant hopes to be seen as a 'Metaverse company' in the future is only one example of how multinational companies are investing billions of dollars into the development of immersive environments that offer a range of activities from socializing and shopping to education and business.[9] Facebook – or now, Meta – are not alone. Microsoft and Google also invest in this cutting-edge technology, alongside other 'non-tech' companies such as Nike, Walmart, Adidas, and PepsiCo.[10] By 2026, it is estimated that a quarter of all consumers will spend at least one hour daily in the Metaverse, and a third of all organizations will have Metaverse-ready products and services.[11]

---

7 Stephenson, Neal. *Snow crash: A novel.* Spectra (2003) p. 24-26.

8 Wang, Y. et al. 'A Survey on Metaverse: Fundamentals, Security, and Privacy'. *IEEE Communications Surveys & Tutorials.* 2022, p. 49; Ball, Matthew. *The Metaverse: And How It Will Revolutionize Everything.* 1st edn. New York: Liveright Publishing Corporation, a division of W.W. Norton & Company (2022).

9 Isaac, Mike, 'Facebook Renames Itself Meta', *The New York Times*, 2021.

10 Drapkin, Aaron, 'Metaverse Companies: Who's Involved and Who's Investing in 2022', *tech.co.* 2023-01-24. https://tech.co/news/metaverse-companies-whos-involved-whos-investing. (Accessed 2023-02-05).

11 Rimol, Meghan, 'Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026'. Press release 2022-02-07. *Gartner.* https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026.

To put this in numbers, the Metaverse is expected to generate up to $5 trillion in value by 2030.[12] Subsequently, the evolution of the Metaverse will likely affect the online activities of consumers and companies substantially.

So, if user data is the product of the current online world, the Metaverse has the potential to make everything and everyone the product.[13] Consolidating the aforementioned emerging technologies allows for manipulating individuals at far deeper levels than currently possible. As the Metaverse expands into various application areas, e.g., healthcare, agriculture, and defense, concerns about privacy rights will be relevant to both government agencies and companies.[14] These technologies are likely to increase the first-hand data collection carried out by governments. Further, private entities may sell or trade the data to governments and simultaneously use it for their purposes.[15] To this background, the ongoing deployment of these technologies calls for an examination of the effects that they may have on human rights and the right to privacy.

---

12 Elmasry, Tarek et al., 'Value creation in the metaverse - The real business of the virtual world', *McKinsey & Company*. 2022-06-14. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse. (Accessed 2023-01-01).

13 Pietro, Roberto Di and Cresci, Stefano. 'Metaverse: Security and Privacy Issues'. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 2021, 281-88.

14 Copeland, Christopher and Michl, Kyle, 'Research Report: Government enters the metaverse', *Accenture Federal Services - Federal Technology Vision 2022*. 2022-09-12. https://www.accenture.com/us-en/insightsnew/us-federal-government/technology-vision-2022. (Accessed 2023-01-25).

15 Regarding data transfer from private companies to government agencies, the activities carried out by the NSA under the PRISM programs is a prominent example of how data, collected by private entities, cannot be expected to remain hidden from governments. See for example Humble, Kristian P. 'International law, surveillance and the protection of privacy'. *The International Journal of Human Rights*. Vol. 25, No. 1. 2021, 1-25; Gellman, Barton and Poitras, Laura, 'NSA slides explain the PRISM data-collection program', *The Washington Post*, 2013.

1.3 Problem statement

In its latest resolution on the right to privacy in the digital age, the UN Human Rights Council reaffirmed that "*the same rights that people have offline must also be protected online.*"[16] The Metaverse represents a cutting-edge digital concept that could revolutionize our interactions with technology. This thesis is specifically concerned with two areas where the Metaverse gives rise to meaningful risks from a human rights perspective: privacy and jurisdiction.

Of the human rights enshrined in international legal frameworks, the right to privacy has been the one most significantly affected by digitalization and technological development.[17] It is established as a human right in the European Convention on Human Rights (ECHR), as well as in EU law and international human rights law.[18] Given the interplay between the evolution of privacy rights and technological advancements, it is of interest to examine how the right to privacy can be affected by the Metaverse. Privacy rights are ultimately manifested as decision rights – individuals have the right to decide where they want to be placed on the spectrum between secrecy and transparency. The Metaverse and its associated technologies could affect such decision rights and might even have the potential to eliminate them. Therefore, it is worth assessing how the interpretation of privacy can evolve to uphold the right to privacy in this context.

Regarding jurisdiction, the Metaverse is a digital space that often transcends national borders. The state parties to the ECHR are obliged to ensure the rights and

16 United Nations General Assembly, *The right to privacy in the digital age - Resolution adopted by the Human Rights Council on 26 September 2019*, 2019. (A/HRC/RES/42/15).

17 See e.g., Holtzman, David H. *Privacy lost: how technology is endangering your privacy.* John Wiley & Sons (2006) p. xix ff.

18 Article 12 of the Universal Declaration of Human Rights (UDHR); Article 17 of the International Covenant on Civil and Political Rights (ICCPR); Article 7 of the Charter of Fundamental Rights of the European Union (2000/C 364/01) (CFR); Article 8 of the The Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (ECHR).

freedoms in the Convention to individuals *within their jurisdiction.*[19] The concept of jurisdiction is commonly linked to the notion of territory, but it is also recognized to exist separately or beyond territorial limitations.[20] The global reach of the Metaverse could give rise to various situations where jurisdiction will be central in determining the practical application of human rights in the virtual context. Typically, the jurisdictional issues arising concerning virtual human rights violations have involved rights such as privacy and freedom of expression. The issues related to these rights are enhanced due to the emergence of the Metaverse technologies and are highly relevant in this context. However, the Metaverse also creates new opportunities for virtual human rights infringements of rights that typically are connected to physical possession or control, such as the prohibition of torture and protection of property. Thus, it is interesting to explore how current models for defining jurisdiction according to the ECHR fit into the Metaverse context and what implications such models might have in protecting human rights in this virtual environment.

1.4 Aim & research questions

The purpose of this thesis is twofold; First, this thesis aims to add to the ongoing discourse surrounding the potential impact of the Metaverse on privacy rights. Second, this thesis seeks to explore how jurisdiction is affected by Metaverse's global nature. Examining both substantive and jurisdictional aspects of human rights in the Metaverse will contribute to a deeper understanding of the potential human rights challenges in this novel context. To achieve the thesis' purpose, the following research questions will serve as the framework for the examination and analysis. All of the research questions are examined from the perspective of the ECHR.

Research Question 1: *How can the Metaverse and its associated technologies affect the interpretation of the right to privacy?*

[19] Article 1 ECHR.

[20] Singh, Ms Neha. 'Criminal Jurisdiction in the Metaverse'. *Journal of Survey in Fisheries Sciences.* Vol. 10, No. 1S. 2023, 4302-07.

Research Question 1 aims to explore and analyze which aspects of the right to privacy are likely to be impacted by Metaverse technologies. The research question is based on the ECHR's position that the right to privacy cannot be fully defined.[21] Consequently, the notion of privacy has evolved following societal and technological development.[22] Therefore, analyzing how the conceptualization of privacy can evolve as a response to the technological development associated with the Metaverse is relevant.

Research Question 2: *How do current models for defining jurisdiction apply to virtual human rights infringements occurring outside the territorial borders of the respondent state?*

Research Question 3: *How do alternative approaches for defining jurisdiction apply to virtual human rights infringements occurring outside the territorial borders of the respondent state, and do they contribute to protecting human rights in the Metaverse context?*

Research Questions 2 and *3* address the jurisdictional aspects of virtual human rights infringements facilitated by Metaverse technologies. The analytical framework outlined herein is not exclusively applicable to the right to privacy. The jurisdictional criteria apply to all rights and freedoms enshrined in the ECHR. While acknowledging that certain human rights are more vulnerable to virtual infringements than others, the analysis, in principle, applies to all virtual human rights violations occurring outside the territory of the respondent state.

The jurisdiction section of this thesis scrutinizes how existing models for determining jurisdiction apply within a highly technological context, such as the Metaverse. The associated implications and risks of these models will also be evaluated. Additionally, a selected number of alternative approaches for defining jurisdiction in cases

21 See e.g., *Bensaid v. the United Kingdom* (2001) ECHR 2001-I, para 47.

22 Bates, Ed. *The evolution of the European Convention on Human Rights: from its inception to the creation of a permanent Court of Human Rights.* Oxford University Press (2010).

of virtual human rights infringements are applied and analyzed within a Metaverse context. These alternative approaches are currently not considered established law. The purpose is to determine their practical suitability for safeguarding human rights in a digital context and explore if they beneficially complement current models.

1.5 Delimitations

The description of the technologies and characteristics of the Metaverse provided in *Chapter 2* is not intended to be exhaustive. The Metaverse is a complex concept from a technical perspective and is ultimately composed of several additional layers and technologies than the ones accounted for in this thesis.[23] The parts described in this thesis have been chosen because they are relevant to grasp the basic concept of the Metaverse or because they are related to privacy or jurisdiction. The impact of blockchain technologies is shortly discussed in *Chapter 2* as it is of fundamental importance to the Metaverse. However, this thesis does not directly discuss how blockchain technologies might affect the right to privacy. Instead, the focus is on centralized versions of the Metaverse, where blockchain technologies are utilized for limited purposes.

Further, the interpretation of the right to privacy is dynamic and "*is not susceptible to exhaustive definition*".[24] Thus, it encompasses many concepts, e.g., private life, privacy, data protection, family life, home, and correspondence. All these aspects are neither relevant in the context of this thesis, nor possible to explore in depth given the time constraints of this project. Thus, a selection of aspects deemed relevant for this topic is explored further in-depth, while others are omitted. The elements chosen in this thesis are not claimed to be an exhaustive examination of how the right to privacy can be affected by Metaverse technologies.

---

[23] See e.g., Radoff, Jon, 'The Metaverse Value-Chain', *Medium.com*. 2021-04-07. https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7. (Accessed 2023-02-07); Park, S. M. and Kim, Y. G. 'A Metaverse: Taxonomy, Components, Applications, and Open Challenges'. *IEEE Access*. Vol. 10. 2022, 4209-51.

[24] *Bensaid v. the United Kingdom*, para 47.

1.6 Methodology

Three research questions serve as the framework for this thesis. Each question presents distinct characteristics and complexities, necessitating different methodological approaches to their analysis. This section outlines the methodological framework employed to examine each question, the theoretical foundations that this thesis builds on, and the material on which the study is based.

Research Question 1 examines how Metaverse technologies affect the interpretation of the right to privacy within the framework of the ECHR. This question is inherently forward-looking. Given the emerging nature of the examined technologies, no case law directly addresses the subject. The topic has been explored to a limited extent in the legal doctrine. Thus, there are limited possibilities to examine the issue only from the traditional sources of law, i.e., using a purely legal dogmatic approach. However, a legal dogmatic methodology will be used to outline how the right to privacy is currently understood and what constitutes traditionally protected interests in the context of Article 8 ECHR. This anchors the analysis in traditional legal sources and represents an internal perspective of the law.[25]

The analysis then proceeds to take an external perspective on the law, incorporating non-legal sources to explore the right to privacy in the Metaverse context. This entails that an interdisciplinary approach is applied to shed light on the law from a different perspective. In practice, a legal phenomenon - the right to privacy - is analyzed in light of the technological research related to the Metaverse. Interdisciplinary research entails that knowledge from other disciplines is 'imported' and compared in a legal context, which makes it possible to examine the law from new perspectives.[26] This approach is deemed appropriate, as supplementing human rights

[25] Smits, Jan, 'What is Legal Doctrine?: On the Aims and Methods of Legal-Dogmatic Research', in Rob Van Gestel, Hans-W. Micklitz, and Edward L. Rubin (eds.), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (Cambridge University Press, 2017) 207-28.

[26] Gräns, Minna, 'Allmänt om användningen av andra vetenskaper inom juridiken', in Maria Nääv and Mauro Zamboni (eds.), *Juridisk metodlära* (2nd edn., Lund: Studentlitteratur, 2018) 429-42, p. 429 f; Sandgren, Claes. *Rättsvetenskap för uppsatsförfattare: ämne, material, metod, argumentation och språk.* 5th edn. Stockholm: Norstedts Juridik (2021) p. 52 ff.

legal research with external perspectives can strengthen the research and allow for consideration of empirical dimensions of the law, such as social and technological factors.[27] This research question further draws on the synthetic theory of law and technology, which emphasizes the need for forward-looking and contextual legal research to ensure that traditionally protected interests remain protected in the face of technological change.[28]

The aforementioned methodological approach entails that material beyond traditional legal sources is used as the foundation for the investigation into the implications of the Metaverse on the right to privacy. Primarily, academic sources from technologically oriented disciplines are used, ensuring a technologically informed approach. To ensure a high quality of this material, peer-reviewed journal articles account for the more significant part of the material reviewed. Additionally, non-academic sources such as forums, blogs, and industrial reports are utilized where warranted. To mitigate any quality concerns arising from these sources, they will primarily be used to highlight the public debate relating to the thesis topic. In combination, the materials described above ensure interaction between the legal sources, the social debate, and technical considerations, thus allowing for a comprehensive analysis of the right to privacy in the Metaverse.

Research Question 2 concerns how current jurisdictional models apply to virtual human rights infringements outside a state's territorial borders. This question deals with the present rather than the future. As it seeks to examine established law in the context of the Metaverse, the analysis is primarily based on the traditional sources of law and carried out following a legal dogmatic approach. This entails using and analyzing legal sources to arrive at an arguably comprehensive understanding of es-

---

27 McLnerney-Lankford, Siobhán, 'Legal methodologies and human rights research: Challenges and opportunities', in Bård-Anders Andreassen, H. O. Sano, and Siobhán Mclnerney-Lankford (eds.), *Research methods in human rights: A handbook* (Cheltenham, United Kingdom: Edward Elgar Publishing, 2017) 38-67, p. 48 ff.

28 Cockfield, Arthur and Pridmore, Jason. 'A Synthetic Theory of Law and Technology'. *Minnesota Journal of Law, Science and Technology (MJLST).* Vol. 8, No. 2. 2007, 475-513; Cockfield, Arthur J. 'Towards a law and technology theory'. *Manitoba Law Journal.* Vol. 30, No. 3. 2003, 383.

tablished law.[29] It can also be employed to suggest changes or criticize the prevailing legal position.[30] The main scope of this question is to define the concept of jurisdiction and determine the extraterritorial reach of the ECHR in a virtual context. The scope of the question will, where warranted, extend to pointing out how Metaverse technologies might challenge the jurisdictional concept in the ECHR. Thus, the ability to suggest changes or present criticism of the prevailing legal position enhances the method's suitability for this question. Using the legal dogmatic methodology as accounted for above is sometimes referred to as legal analytical methodology.[31] Others argue that it is within the framework of the legal dogmatic methodology.[32] However, the distinctions in semantics regarding the methodological framework are not further emphasized.

To interpret the ECHR, both in relation to *Research Questions 1* and *2*, the primary material used is the case law of the European Court of Human Rights (ECtHR). The interpretive methods employed by the Court are mainly textual and teleological, which follow the rules of interpretation in Article 31 of the Vienna Convention on the Law of Treaties (VCLT).[33] This means that terms are interpreted following the ordinary meaning of the words in their context and in light of their objectives and purpose.[34] To this background, the same interpretative methods will be employed throughout this thesis. Further, the Court's reference to the VCLT means that account is to be taken of "*any relevant rules of international law applicable in the relations between the parties*".[35] To this background, the traditional primary

---

29 Kleineman, Jan, 'Rättsdogmatisk metod', in Maria Nääv and Mauro Zamboni (eds.), *Juridisk metodlära* (2nd edn., Lund: Studentlitteratur, 2018) 21-47, p. 21-26.

30 Smits, 'What is Legal Doctrine?: On the Aims and Methods of Legal-Dogmatic Research', in Gestel, Micklitz, and Rubin (ed.).

31 Sandgren, Claes. 'Är rättsdogmatiken dogmatisk?'. *Tidsskrift for Rettsvitenskap.* Vol. 118, No. 4/05. 2006, 648-56.

32 Kleineman, 'Rättsdogmatisk metod', in Nääv and Zamboni (ed.), p. 36 ff.

33 To the Courts' acceptance of the Vienna Convention rules as interpretation guidelines, see *Golder v. the United Kingdom* (1975) Series A No. 18.

34 Cameron, Iain. *An introduction to the European Convention on Human Rights.* 8th edn. Uppsala: Iustus (2018) p. 80-81.

35 *Al-Adsani v. the United Kingdom* (2001) ECHR 2001-XI, para 55.

sources of international law – international conventions, international customary law, and general principles – can be considered where warranted.[36] Given that the right to privacy is also enshrined in Article 12 of the ICCPR, case law from the ICJ and the HR Committee might be used for illustrative purposes. These sources are further complemented by legal doctrine.

Research Question 3 proceeds to analyze a number of alternative approaches to defining jurisdiction and evaluate their potential contribution to protecting human rights in the Metaverse context. The material used to answer this research question is derived from legal sources. The jurisdictional approaches examined are (1) the 'third' approach, (2) the virtual approach, and (3) the functional approach. The two former stem from journal articles by Marko Milanovic and Peter Margulies, written in response to the Edward Snowden revelations, and concern jurisdiction in cases of virtual human rights infringements. Thus, they are part of the legal doctrine. The last approach is based on Judge Bonello's separate opinion in *Al-Skeini v. UK* and is derived from case law.

Whether the methodology employed to address this research question can be categorized as legal dogmatics can be debated. While it is evident that the analysis draws on legal sources, the approach does not intuitively align with the principles of legal dogmatics. The alternative approaches examined have not been applied to virtual human rights infringements and hence cannot be considered established law. Also, this research question does not aim to arrive at a definitive interpretation of established law. Such a goal is instead pursued in *Research Question 2*. The primary objective of this question is to examine the potential of alternative approaches to address the inadequacies of current jurisdictional approaches in managing virtual human rights infringements. Therefore, the efficiency of the alternative approaches in remedying the deficiencies of existing jurisdictional frameworks is a central focus of this question. The analysis conducted in this section does not neatly fit under a suitable methodological label. Hence, the above description is deemed sufficiently transparent to give the reader an understanding of the practical method used to

[36] Article 38(1) Statue of the International Court of Justice.

address the research question. The alternative approaches considered are of high quality, proposed by prominent scholars, well-cited, and highly relevant to the topic. Therefore, they constitute an appropriate starting point for examining alternative ways of managing jurisdictional issues in the era of the Metaverse.

1.7 Prior research & contribution

The potential effect of Metaverse technologies on the conceptualization of the right to privacy has been examined to a limited extent in the legal doctrine. However, some works should be noted. First, the book *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse* by Elizabeth Renieris must be mentioned.[37] The book has inspired this thesis and provides numerous nuanced discussion points about privacy in the cyber-physical world. Further, Brittan Heller commendably describes the effect of immersive technologies and biometric psychography on privacy in her article *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law.*[38] Jan-Christoph Bublitz's analysis on the right to psychological integrity in light of emerging technologies provided great insight into how the complexity of regulating the human mind can be managed.[39] In addition, the privacy implications of the Metaverse have been examined more in scientific literature, which has been used to link the technical privacy perspectives to the legal ones.[40]

---

37 Renieris, Elizabeth M. *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse.* MIT Press (2023).

38 Heller, Brittan. 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law'. *Vand. J. Ent. & Tech. L.* Vol. 23. 2020, 1-51.

39 Bublitz, Jan-Christoph, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Andreas Von Arnauld, Kerstin Von Der Decken, and Mart Susi (eds.), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (Cambridge: Cambridge University Press, 2020) 387-403.

40 See e.g., Pietro and Cresci, 'Metaverse: Security and Privacy Issues'; Huang, Y., Li, Y. J., and Cai, Z. 'Security and Privacy in Metaverse: A Comprehensive Survey'. *Big Data Mining and Analytics.* Vol. 6, No. 2. 2023, 234-47; Wang et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy'.

The jurisdictional issues surrounding the Metaverse have been addressed to a minimal extent in the legal doctrine.[41] However, the legal implications of foreign mass surveillance, which involves using digital technologies to commit human rights violations remotely, have been extensively discussed in legal doctrine since the Edward Snowden revelations in 2013. These discussions offer valuable insights into the potential jurisdictional challenges of the Metaverse. With inspiration from Erica Wide's master thesis *Exporting Privacy - A Study on the Extraterritorial Application of the European Convention on Human Rights to Foreign Mass Surveillance*, a number of articles on foreign mass surveillance were identified.[42] These sources, in combination with several others, have served as the basis for the conducted analysis. Marko Milanovic's article Human rights treaties and foreign surveillance: Privacy in the digital age,[43] Holly Huxtables article *E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance*,[44] Eliza Watt's article *The role of international human rights law in the protection of online privacy in the age of surveillance*,[45] and Peter Margulies' article *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*[46] has been especially important. By drawing on these sources, this thesis explores the potential challenges surrounding jurisdiction in the Metaverse and highlights how the legal implications of extraterritorial jurisdiction are relevant to this discussion.

---

41 See however Singh, 'Criminal Jurisdiction in the Metaverse'; Kalyvaki, Maria. 'Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction'. *Journal of Metaverse*. Vol. 3, No. 1. 2023, 87-92.

42 Wide, Erica, 'Exporting Privacy - A Study on the Extraterritorial Application of the European Convention on Human Rights to Foreign Mass Surveillance' (Master Thesis, Lund University, 2020).

43 Milanovic, Marko. 'Human rights treaties and foreign surveillance: Privacy in the digital age'. *Harvard International Law Journal*. Vol. 56. 2015, 81-146.

44 Huxtable, Holly. 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance'. *Security and Human Rights*. Vol. 28, No. 1-4. 2018, 92-112.

45 Watt, Eliza. 'The role of international human rights law in the protection of online privacy in the age of surveillance'. *2017 9th International Conference on Cyber Conflict (CyCon)*. 2017, 1-14.

46 Margulies, Peter. 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism'. *Fordham L. Rev.* Vol. 82. 2013, 2137.

The concept of the Metaverse has received limited discussion from a human rights perspective. This thesis builds on technological literature and adds to the current debate on how the right to privacy can be understood in the Metaverse era. Further, it draws on literature about the ECHR's extraterritorial application in foreign mass surveillance cases to analyze how Metaverse technologies will amplify the jurisdictional complexity when dealing with virtual human rights violations. This thesis will contribute to a deeper understanding of the potential human rights challenges in this novel context by examining both substantive and jurisdictional aspects of human rights in the Metaverse.

1.8 Disposition

This thesis is divided into six chapters. *Chapter 1* introduces the Metaverse and contextualizes the issue the thesis aims to analyze. Also, it summarizes the prior research on this topic and the intended contribution of this thesis. *Chapter 2* defines the Metaverse for the purposes of this thesis. It also outlines key characteristics and technologies relevant to the research questions. *Chapter 3* corresponds to *Research Question 1* and thus focuses on the substantive definition of the right to privacy. *Chapter 4* corresponds to *Research Questions 2* and *3* and thus focuses on jurisdiction in cases of virtual human rights infringements facilitated by Metaverse technologies. First, the nature of virtual human rights infringements in the Metaverse is explained and exemplified. Then, the interpretation of jurisdiction in the ECtHR's case law and the existing models for extraterritorial application is applied and analyzed in the Metaverse context. Further, the application of alternative models is considered and analyzed. *Chapter 5* presents the conclusions and answers to the research questions. *Chapter 6* discusses perspectives on the research questions derived from reflections during the thesis project but that are not subject to a thorough academic analysis. It also proposes areas for further research.

2 The Metaverse

In the context of this thesis, it is imperative to have a clear understanding of what the Metaverse entails. This chapter provides a concise overview of its essential characteristics and offers a definition of the Metaverse for the purposes of this thesis. Further, a selection of key technologies is briefly explained.

2.1 What is the Metaverse?

Given the lack of a universal definition for the still-evolving concept of the Metaverse, the definitions used in academic and non-academic literature can be perceived as fragmented. However, a selection of sources deemed sufficient to summarize the key aspects of the concept of the Metaverse has therefore been chosen as the basis for a definition for the purposes of this thesis. In his book *The Metaverse: And how it will revolutionize everything*, Matthew Ball defines the Metaverse as:

> *A massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments.*[47]

In academic literature, Park & Kim reviewed 230 Metaverse-related articles and described the Metaverse as:

> *Metaverse is a compound word of transcendence meta and universe and refers to a three-dimensional virtual world where avatars engage in political, economic, social, and cultural activities. It is widely used in the sense of a virtual world based on daily life where both the real and the unreal coexist.*[48]

---

[47] Ball, *The Metaverse: And How It Will Revolutionize Everything*, p. 49.

[48] Park and Kim, 'A Metaverse: Taxonomy, Components, Applications, and Open Challenges'.

Similarly, Lee et al. describe the Metaverse as:

> *(...) a virtual environment blending physical and digital, facilitated by the convergence between the Internet and Web technologies, and Extended Reality (XR).*[49]

Based on these definitions, a definition for the purposes of this thesis is offered. The Metaverse will be understood as a virtual world composed of computer-generated elements, including user-controlled avatars, digital objects, and virtual environments, where people (represented by their avatars) can communicate, collaborate, and socialize in real-time. This world is characterized by its scale and interoperability, allowing for a potentially unlimited number of users to engage in various activities.

In addition to being a virtual world, the Metaverse can also refer to the collection of technologies used to create it. These technologies primarily include immersive technologies like XR, VR, AR, and MR, as well as artificial intelligence and blockchain. Where warranted, these technologies are considered independent of the Metaverse, particularly when they significantly impact issues relating to privacy or jurisdiction. In cases where a particular technology is a determining factor in such matters, it may warrant a separate discussion and analysis.

2.2 Key characteristics of the Metaverse

The Metaverse is composed of several layers, technologies, and application areas. In this section, key characteristics of the Metaverse that are relevant to the research questions are described more in-depth.

2.2.1 Interoperability

Interoperability is expected to catalyze the growth and development of the Metaverse. It entails that users can easily transition between virtual worlds (sub-metaverses)

[49] Lee, Lik-Hang et al. 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda'. *arXiv preprint arXiv:2110.05352.* 2021.

without disrupting their immersive experience.[50] Digital assets used for creating or recreating virtual worlds (e.g., NFTs, digital currency) are compatible across different platforms.[51] Different applications, e.g., finance and healthcare, can communicate and exchange information seamlessly. Virtual bridges will be created to facilitate this, enabling users to transfer their avatars and possessions between virtual worlds. Additionally, a unique set of credentials will be issued to each user based on an identity standard, and these credentials will be usable across virtual world borders.[52] This is expected to be equivalent to real-life identification numbers such as license numbers, social security numbers, passport numbers, and other forms of identification. To facilitate interoperability, even centralized Metaverse versions are expected to include decentralized features, particularly of economic character. For instance, Horizon Worlds (Meta's version of the Metaverse) will likely be centrally controlled by Meta, but utilize blockchain technology to enable transactions within the Metaverse and allow users to transfer their digital assets between other sub-metaverses.

2.2.2 (De)centralization

A centralized Metaverse is a virtual world centrally managed and controlled by a single entity or organization. All aspects of the Metaverse, such as the user experience, content creation, and governance, are controlled by this central authority. Examples of centralized Metaverses are those currently developed by big tech firms, such as Horizon Worlds (developed by Meta) and Mesh (developed by Microsoft). Centralized Metaverses can still include decentralized elements, such as blockchain and NFT technology, to facilitate a complete digital economic environment. Thus, the degree of decentralization and blockchain implementation in a Metaverse can be viewed as a spectrum rather than a binary option.[53] However, a significant difference

---

50 Ibid.

51 Dionisio, John David N, III, William G Burns, and Gilbert, Richard. '3D virtual worlds and the metaverse: Current status and future possibilities'. *ACM Computing Surveys (CSUR)*. Vol. 45, No. 3. 2013, 1-38.

52 Stokel-Walker, Chris. 'Welcome to the Metaverse'. *New Scientist*. Vol. 253, No. 3368. 2022, 39-43.

53 Johnson, Shawn, 'Centralized and Decentralized Metaverse: What's the Difference?', *BusinessNews*. 2023-01-22.

is that in centralized Metaverses, the user data is typically held by the controlling entity, such as governments or corporations. This means that these entities have complete control over individuals' data and can, from a technical perspective, use it without the individual's knowledge or consent.[54]

In contrast, a decentralized Metaverse is a virtual world based on decentralized technologies, i.e., blockchain. Decentralization means that no single entity has control over the Metaverse. Its operations are instead managed by a distributed network of multiple computers known as nodes. In a decentralized Metaverse, users have more control over their data and assets. Instead of being stored in a single location, data is stored on multiple nodes that are part of the blockchain network. Every node has a copy of the same information, and each new addition to the blockchain requires approval from each node.

Because of the distributed nature of the blockchain, data is highly secure, and it is almost impossible to tamper with it or add fraudulent entries to the ledger. Individuals can control their data by deciding which information they want to store on the blockchain, who can access it, and for what purposes. They can also monitor who has accessed their data and ensure that their data is not being used in ways they disapprove of.[55] Decentralized Metaverses typically build on a system called DAO, meaning that smart contracts set the rules for a specific Metaverse. Examples of decentralized Metaverses include The Sandbox and Axie Infinity, which utilize a play-to-earn model that allows users to earn tokens or cryptocurrency through gameplay. Another example is Decentraland, which follows a more conventional approach where users own and trade virtual plots of land.

---

https://biz.crast.net/centralized-and-decentralized-metaverse-whats-the-difference-cryptosaurus/. (Accessed 2023-05-12).

[54] Rodriguez, Katitza and Mir, Rory, 'Pivotal Year for the Metaverse and Extended Reality: 2022 in Review', *The Electronic Frontier Foundation (EFF)*. 2022-12-24. https://www.eff.org/deeplinks/2022/12/pivotal-year-metaverse-and-extended-reality. (Accessed 2023-05-12).

[55] Conoscenti, M., Vetrò, A., and Martin, J. C. De. 'Blockchain for the Internet of Things: A systematic literature review'. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. 2016, 1-6.

2.2.3 Avatars

An individual participates in Metaverse activities through their Metaverse avatar. The avatar functions as a user's identity in the entire universe and is the virtual embodiment of the user. The avatar has the same legal authority in the Metaverse as the individual has in the real world. Thus, the avatar is warranted for any transactions made within the virtual world and restricts the individual from repudiating any committed action.[56]

2.2.4 Internet of Things (IoT) and smart cities

In simple terms, IoT refers to connecting everyday objects to the internet so that they can communicate and exchange information with each other and with people. The data collected from these devices can be analyzed and used to make informed decisions, automate tasks, and improve efficiency in industries like healthcare, manufacturing, and transportation. From a more technical perspective, IoT is a network of physical devices, vehicles, appliances, and other items embedded with electronics, software, sensors, and connectivity, which allows them to exchange data with other devices and systems over the internet.[57] IoT is used in the Metaverse context to provide users with immersive cyber-virtual experiences in extended reality environments.[58]

In other words, the IoT can be used in the Metaverse to create better digital experiences. Real-life information from IoT devices can be brought into the virtual world, making it more realistic.[59] For example, the IoT can help virtual purchasing experiences, such as virtual fitting rooms. XR devices can be used to track the movement of the user's body. The personal body information could be updated through data

[56] Gadekallu, Thippa Reddy et al. 'Blockchain for the metaverse: A review'. *arXiv preprint arXiv:2203.09738.* 2022.

[57] Dorsemaine, B. et al. 'Internet of Things: A Definition & Taxonomy'. *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies.* 2015, 72-77.

[58] Li, Kai et al. 'When Internet of Things Meets Metaverse: Convergence of Physical and Cyber Worlds'. *IEEE Internet of Things Journal.* 2022.

[59] Kanter, Theo. 'The metaverse and extended reality with distributed IoT'. *IEEE Internet of Things Magazine.* 2021.

from photos taken on the user's smartphone or smart weighing scales. Users in the Metaverse are thus able to fully immerse in a virtual representation of the store and overcome some of the barriers associated with traditional online shopping, e.g., the inability to try on the clothes you are buying.[60]

Smart cities use technology to improve the quality of life for their residents. IoT devices are often used in smart cities to collect data and help with things like traffic management and waste management.[61] Similarly, IoT devices can be used in the Metaverse to create a more realistic and immersive experience. For example, if a city has smart traffic lights, this data could be reflected in the Metaverse to show traffic patterns in real-time. By connecting the Metaverse and IoT to smart cities, it is possible to create a more seamless and integrated experience between the physical and virtual worlds.

2.3 Technologies of the Metaverse

In this section, a selection of technologies that are essential in the development of the Metaverse is presented. They provide the infrastructure and tools to build, manage, and interact with the virtual world.

2.3.1 Immersive technologies

Immersive technologies, also referred to as extended reality (XR), is an umbrella term for virtual reality (VR), augmented reality (AR), and mixed reality (MR). Immersive technologies, as described below, allow for immersive and interactive experiences in the Metaverse. Combined, all these technologies provide the capability to blend physical and digital environments seamlessly.

60 Li et al., 'When Internet of Things Meets Metaverse: Convergence of Physical and Cyber Worlds', p. 2-3.

61 Green, Ben. *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future.* Ideas Series Cambridge: The MIT Press (2019) p. 92.

Virtual reality (VR) - A technology that uses a device worn on the body, such as a VR headset, to place the user inside an interactive virtual environment.[62]

Augumented reality (AR) - A technology that adds digital content to a user's visual plane by overlaying digital objects on top of real-life objects (e.g., Pokémon Go). These digital assets do not interact with the user's environment.[63] For example, a puppy showed in AR would be seen as layering over a table in the user's environment, but it would not recognize the table as a surface to go around or sit on.[64]

Mixed Reality (MR) - MR combines VR and AR experiences by displaying virtual and actual environments together and allowing computer-generated objects to interact with real-life objects.[65] In MR, the virtual puppy can go under the tabletop and around its legs.

These technologies play a vital role in providing the illusion of presence and enabling users to interact with digital objects and environments as if they were real. This level of immersion and interaction will be the foundation for building the Metaverse.

Immersive technology hardware is the tool used to access the Metaverse. In practice, immersive technologies are implemented into hardware devices used to create and enhance the user's experience in virtual environments. The clearest examples are AR and VR glasses like Microsoft HoloLens and Oculus Quest. The development of such hardware plays a crucial role in the Metaverse development. For example, HoloLens 2 has been deemed essential in taking the Metaverse from gaming and

62 Park and Kim, 'A Metaverse: Taxonomy, Components, Applications, and Open Challenges'.

63 Avila, Sandra. 'Implementing augmented reality in academic libraries'. *Public Services Quarterly.* Vol. 13, No. 3. 2017, 190-99.

64 Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law'.

65 Park and Kim, 'A Metaverse: Taxonomy, Components, Applications, and Open Challenges'.

entertainment into productivity and education.[66] Further, haptic sensors integrated into gloves, keyboards, and other wearables, can provide kinetic feedback to the user. Expected future development in this field includes combining AR glasses and cameras, allowing human communication to be simulated by replicating eye movements, breathing patterns, double takes, and other nonverbal cues.[67] Additionally, cameras can map the user's facial movements onto a photorealistic avatar or a digitally rendered image, creating the illusion of being on camera when actually wearing a VR or AR headset. Wearable haptic sensors can further amplify the nonverbal signals that the user transmits to their conversation partner.

2.3.2 Artificial intelligence

AI plays a significant role in the development and operation of the Metaverse. AI can be used in several ways to enhance the user experience, make virtual environments more immersive, and provide advanced functionality. As described by Wang et al., AI acts as the brain of the Metaverse.[68] It enables customized and personalized experiences through features such as personalized avatar creation and multilingual support by analyzing vast amounts of data.[69]

Also, AI facilitates smart interactions between users and NPCs. AI algorithms can continuously learn from a user's facial expressions, emotions, and other traits to create personalized NPCs and provide intelligent recommendations for goods or information within the Metaverse.[70] AI is used in the Metaverse to carry out predictive analytics, meaning that it analyzes data from the Metaverse to predict user behavior. This is essential in the business model employed by big tech firms.[71]

---

66 Feltham, Jamie, 'HoloLens 2 Review: Ahead Of Its Time, For Better And Worse', *Upload.* 2021-04-09. https://www.uploadvr.com/hololens-2-review/. (Accessed 2023-05-12).

67 Garon, Jon. 'Legal implications of a ubiquitous metaverse and a Web3 future'. *Marq. L. Rev.* Vol. 106. 2022, 163, p. 167.

68 Wang et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy'.

69 Ibid.

70 Huynh-The, Thien et al. 'Artificial intelligence for the metaverse: A survey'. *Engineering Applications of Artificial Intelligence.* Vol. 117. 2023.

71 Zuboff, 'Big Other: surveillance capitalism and the prospects of an information civilization'.

2.3.3 Blockchain

Blockchain technology[72] is a cornerstone in Metaverse development. The concept of blockchain technology originated from a white paper by Satoshi Nakamoto in 2008.[73] It is a form of digital ledger comprising consecutive blocks linked together through a cryptographic hash value.[74] The functioning of blockchain technology is maintained by every node in the network being required to follow a common consensus protocol, which regulates its operating principles and legitimate actions.[75] As discussed in *Section 2.2.2*, the degree of implementation of blockchain technology distinguishes decentralized Metaverses from centralized ones. Apart from this, blockchain technology is essential for two purposes.

First, blockchain technology acts as a repository, allowing users to store data anywhere in the Metaverse.[76] Second, blockchain is crucial for the Metaverse economy. The decentralized and secure nature of blockchain technology provides a foundation for the virtual economy of the Metaverse, allowing for seamless transactions and asset ownership. Without blockchain support, the economy of the Metaverse would be susceptible to control by a single entity. This would make it difficult to establish the value of resources and goods within the Metaverse and to facilitate economic transactions comparable to those in the real world.[77]

---

72 This explanation of blockchain is indented to be of summarizing character. For further reading, please refer to the referenced literature.

73 Nakamoto, Satoshi. 'Bitcoin: A peer-to-peer electronic cash system'. *Decentralized Business Review.* 2008, 21260.

74 Huo, Ru et al. 'A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges'. *IEEE Communications Surveys & Tutorials.* Vol. 24, No. 1. 2022, 88-122.

75 Dotan, Maya et al. 'Survey on blockchain networking: Context, state-of-the-art, challenges'. *ACM Computing Surveys (CSUR).* Vol. 54, No. 5. 2021, 1-34.

76 Gadekallu et al., 'Blockchain for the metaverse: A review'.

77 Hyun-joo, Jeon et al., 'Blockchain and AI Meet in the Metaverse', in M. Fernández-Caramés Tiago and Fraga-Lamas Paula (eds.), *Advances in the Convergence of Blockchain and Artificial Intelligence* (Rijeka: IntechOpen, 2021) Ch. 5, p. 78-79.

3 Privacy in the Metaverse

This chapter details the development and characteristics of the right to privacy. This chapter then proceeds to analyze the right to privacy in the Metaverse context.

3.1 A regular day in the Metaverse

In our everyday lives, technology accompanies us from the moment we wake up until we go to sleep. These interactions with technology can, and probably will, transition into the Metaverse. Video conferencing tools will evolve into lifelike holographic meetings, where participants can gather virtually in the same room. Social media will transform from scrolling through news feeds to virtual communities for real-time conversations. Online shopping will become multidimensional, allowing us to try on virtual clothing before making a purchase. Gaming currently pioneers this transformation by moving into fully immersive, hyper-realistic simulations.

Consider, then, that you attend a virtual work meeting in the Metaverse. During your meeting, a promotion you've been hoping for is discussed, and your body responds with excitement - your heart rate increases, and your pupils dilate. Later at night, you play a virtual reality game with your friends. As you play, your adrenaline spikes, and your pulse is heightened. As you engage in these virtual experiences, the technology constantly records and analyzes your behavior and reactions to stimuli, including your involuntary biological responses. This information can – for example - be used to monitor your work performance and predict your political leanings, views on social issues, and voting patterns. The data holder can target you with propaganda, influence your opinions, or even interfere with elections. In the words of Brittan Heller, engaging in Metaverse activities is comparable to "*hitting a like button on steroids*".[78]

[78] For the inspiration to this example, see Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law'.

3.1.1 Introduction to the right to privacy

The right to privacy is a human right that has been increasingly recognized and protected by law in recent decades. In 1948, in the aftermath of World War II, the UN General Assembly adopted the Universal Declaration of Human Rights (UDHR), which declared privacy as a human right.[79] This was the first time *privacy* was explicitly used as a concept encompassing protection for one's family, home, and correspondence from intrusions from the state.[80] In the ECHR, the right to respect for private and family life is enshrined in Article 8. The right is qualified rather than absolute, which implies that the right may be restricted. Any limitations must be laid out in detailed and specific legislation that outlines precisely when and to what extent the right to privacy can be compromised.[81] This is clearly expressed in the text of the ECHR, which specifies that the right may be interfered with only if (1) the interference is "*in accordance with the law*", (2) the interference serves a "*legitimate aim*", and (3) such interference is "*necessary in a democratic society*".[82] It should be noted that where UDHR and ICCPR use the phrase 'privacy', the Convention uses 'private (...) life'. This does not reflect any difference in substance.[83] Accordingly, the terms 'privacy' and 'private life' are used interchangeably in this thesis.

---

79 Article 12 UDHR.

80 Diggelmann, Oliver and Cleis, Maria Nicole. 'How the right to privacy became a human right'. *Human Rights Law Review*. Vol. 14, No. 3. 2014, 441-58.

81 Kindt, Els J., 'The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing', in Pompeu Casanovas and Giovanni Sartor (eds.), *Privacy and Data Protection Issues of Biometric Applications - Part of the Law, Governance and Technology Series book series* (Dordrecht: Springer Netherlands, 2013) 403-567, p. 453-54.

82 See Article 8 ECHR. Other qualified rights in the ECHR are the right to a fair hearing in Article 6(1), the presumption of innocence in Article 6(2) (while these rights are not qualified in express terms, the ECtHR has held that these rights are subject to limitations, see e.g., *Naït-Liman v. Switzerland* (2018) [GC] ECHR 2018, para 113-15.), the right to freedom to manifest one's religion in Article 9, the right to freedom of expression in Article 10, and the right to freedom of peaceful assembly and association in Article 11.

83 Merrills, J. G. and Robertson, A. H. Human rights in Europe: A study of the European Convention on Human Rights (*e-book*). 4th edn. Manchester: Manchester University Press (2022) Section '*Article 8: The right to respect for private and family life, home and correspondence*'.

To this date, there is no generally recognized definition of privacy.[84] At its core, the right to privacy builds on two concepts.[85] On the one hand, privacy is about freedom, i.e., creating distance between an individual and the state, allowing the individual to be left alone from state interventions. On the other hand, privacy is about dignity, i.e., safeguarding essential societal values, such as personal relationships and public reputation. Historically, the American legal tradition has prioritized the freedom aspect of privacy, while the European tradition has emphasized the dignity aspect.[86]

Nevertheless, both perspectives are included in the Convention, as reflected in the wording of Article 8 ECHR.[87] The difficulties in formulating an exhaustive definition of the right to privacy are connected to the fact that the interpretation of the right is dynamic, in the sense that its meaning can evolve to correspond to technical and societal changes.[88] In *Bensaid v. UK*, the Court explicitly stated that the notion of 'private life' is 'not susceptible to exhaustive definition.[89]'This implies that the right to privacy encompasses multiple aspects that have evolved through the EctHR's case law development. The remainder of this section is devoted to briefly presenting the development and scope of Article 8 ECHR. The various aspects of the right to privacy can be conveniently classified into four distinct categories: (1) privacy, (2) family life, (3) home, and (4) correspondence.[90]

---

84 Diggelmann and Cleis, 'How the right to privacy became a human right'; Solove, Daniel J. 'A Taxonomy of Privacy'. *University of Pennsylvania Law Review*. Vol. 154, No. 3. 2006, 477-564.

85 Whitman, James Q. 'The Two Western Cultures of Privacy: Dignity versus Liberty'. *The Yale Law Journal*. Vol. 113, No. 6. 2004, 1151-221.

86 Ibid.

87 See e.g., the phrasing "there shall be no interference by a public authority with the exercise of this right..." in Article 8(2) ECHR.

88 Bates, *The evolution of the European Convention on Human Rights: from its inception to the creation of a permanent Court of Human Rights.*

89 *Bensaid v. the United Kingdom*, para 47.

90 Merrills and Robertson, Human rights in Europe: A study of the European Convention on Human Rights (*e-book*), Section '*Article 8: The right to respect for private and family life, home and correspondence*'.

Many actions can simultaneously interfere with several aspects, e.g., an action can violate the right to respect for home and correspondence, and concurrently interfere with the right to family life.[91] This highlights the relation between the various parts of Article 8 ECHR. The four categories are visualized below in *Figure 3.1.*

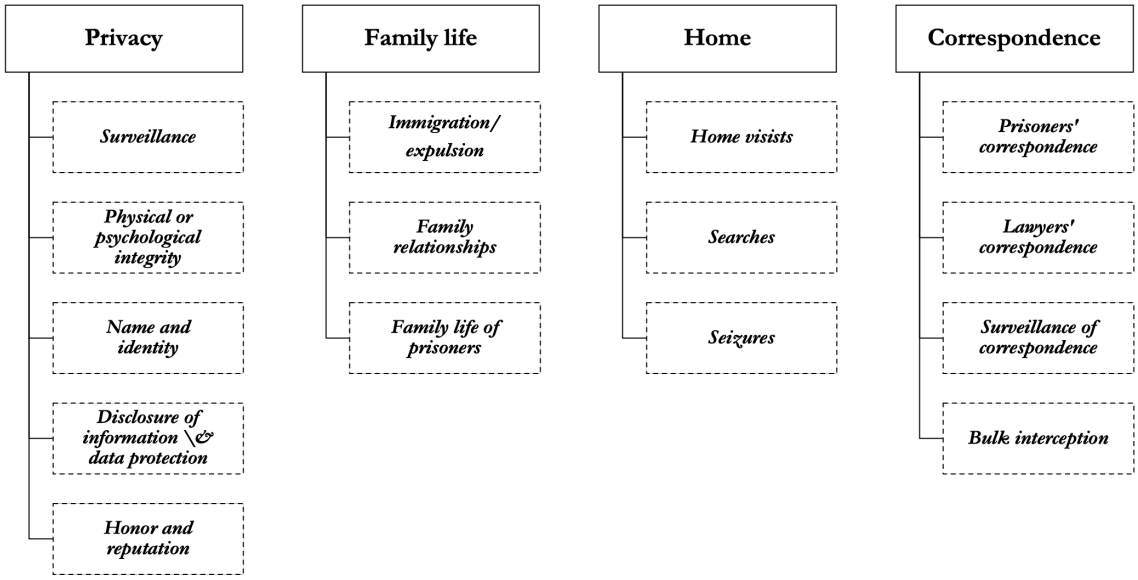

Figure 3.1: Categories of the right to privacy based on Merrills and Robertson (2022).

An introduction to each category is given below. This account is purely descriptive and intends to provide the reader with a basic understanding of the different aspects of the right to privacy, before analyzing how these relate to the Metaverse.

3.1.2 Privacy

The notion of privacy is not susceptible to an exhaustive definition. However, it has been argued that five distinct elements of privacy can be identified, outlined below.[92]

---

91 *Lüdi v. Switzerland* (1992) Series A No. 238; *Klass and Others v. Germany* (1978) Series A No. 28.

92 Loucaides, Loukis G, 'Personality and Privacy under the European Convention on Human Rights', in Loukis G Loucaides (ed.), *Essays on the Developing Law of Human Rights* (Brill Nijhoff, 1995) 83-107, p. 177; Merrills and Robertson, Human rights in Europe: A study of the European Convention on Human Rights (*e-book*), Section '*Privacy*'.

I. Protection against being spied upon, watched, or harassed. If the authorities conduct surveillance such as maintaining records of activities or financial affairs, telephone tapping, or checking an individual's mail, it typically constitutes an interference with the right to privacy.[93]

II. Protection of one's physical or mental integrity or moral or intellectual freedom. Physical integrity is included is a part of an individual's private live as a person's body concerns the most intimate aspect of private life.[94] However, 'psychological integrity' has been scarcely addressed by the Court and remains largely undefined.

III. Protection of an individual's name, identity or likeness against unauthorized use. Names relate to an individual's private and family life as a means of personal identification and of linking to a family.[95] If a state attempts to change someone's name or create discriminatory legislation regarding names, it can constitute a violation of Article 8. Since naming practices differ across the member states, they have a wide margin of appreciation in this regard.

IV. Protection against disclosure of information covered by the duty of professional secrecy. If information relating to an individual is released without adequate justification, it typically constitutes an infringement of the right to privacy. Often, issues relating to this aspect of the right to privacy have concerned the release of medical records to third parties.[96] To this, the right to the protection of personal data can be added. The Court has acknowledged that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private life as guaranteed by Article 8 of the Convention.[97]

V. Protection against attacks on an individual's honor or reputation. An attack on an individual's reputation must amount to a certain level of seriousness and be made in a way that causes prejudice to the enjoyment of the right to respect for private life.[98] This pertains to both social and professional reputation.[99]

---

93 Merrills and Robertson, Human rights in Europe: A study of the European Convention on Human Rights (*e-book*), Section '*Privacy*'.

94 *Niemietz v. Germany* (1992) Series A No. 251-B; *Sentges v. the Netherlands* (2004) App No. 27677/02 (ECtHR 8 July 2003); *Pentiacova and Others v. Moldova* (2005) ECHR 2005-I; *Tysiac v. Poland* (2007) ECHR 2007-I.

95 *Burghartz v. Switzerland* (1994) Series A No. 280-B.

96 *Z v. Finland* (1997) Reports of Judgments and Decisions 1997-I; *M.S v. Sweden* (1997) Reports of Judgments and Decisions 1997-IV.

97 *Z v. Finland*; *M.K. v. France* (2005) App. No. 19522/09 (ECtHR 18 April 2013); *S and Marper v. the United Kingdom* (2008) ECHR 2008; *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland* (2017) ECHR 2017 (extracts).

98 *Axel Springer AG v. Germany* (2012) [GC] App. No. 39954/08 (ECtHR 7 February 2012)

99 *Denisov v. Ukraine* (2018) [GC] App. No. 76639/11 (ECtHR 25 September 2018).

3.1.3 Family life

The protection of the right to family life encompasses a wide range of circumstances. The definition of 'family' should be interpreted broadly to include married couples and their children, adopted children, stepchildren, and other relatives living together.[100] Article 8 and Article 12 ECHR are closely related, as the latter concerns the right to marry and establish a family.[101] Issues related to family life include parent-child relationships, such as legal issues regarding illegitimate children, decisions concerning the admission or expulsion of family members from a member state, or determining the extent of a prisoner's family life.[102]

3.1.4 Home

Compared to the other categories, there is relatively limited case law related to protecting the right to respect for one's home. While the interests being safeguarded here are narrower than those of privacy and family life, the three often overlap.[103] Typically, interference with the right to respect for one's home occurs when officials enter the home without the occupant's consent.[104] The interpretation of what qualifies as a 'home' for the purposes of the right has been broad.[105]

---

100 *Abdulaziz, Cabales and Balkandali v. UK* (1985) Series A No. 94

101 *Johnston and Others v. Ireland* (1986) Series A No. 112.

102 *X. v. the Federal Republic of Germany* (1970) No. 3603/68, Commission decision of 4 February 1970, Collection of Decisions, 31, pp. 48-50; *Marckx v. Belgium* (1979) Series A, No. 31; *Abdulaziz, Cabales and Balkandali v. UK.*

103 Merrills and Robertson, Human rights in Europe: A study of the European Convention on Human Rights (*e-book*), Section '*Inviolability of the home*'.

104 *Funke v. France* (1993) Series A No. 256-A; Gutsanovi v. Bulgaria (2013) ECHR 2013 (extracts); *Buck v. Germany* (2005) ECHR 2005-IV

105 *Winterstein and Others v. France* (2013) App. No. 27013/07 (ECtHR 17 October 2013); *Chiragov and Others v. Armenia* (2015) [GC] ECHR 2015.

3.1.5 Correspondence

The most typical example of freedom of correspondence is the protection against having one's mail unjustifiably opened by the authorities.[106] However, it also includes situations where no correspondence, e.g., the writing of a letter, has occurred because the interference consists of preventing correspondence from taking place.[107] Further, 'correspondence' is not limited to traditional mail, but also includes communication carried out through technical means, e.g., telephone calls, e-mail, and other electronic communications.[108]

3.2 The Metaverse's effect on the right to privacy

In this section, a number of concepts that are included in the right to privacy are analyzed in the Metaverse context. The different interests behind the right to privacy sometimes overlap, and the Metaverse technologies under analysis are largely interdependent. Thus, while it will be avoided to the extent possible, some repetition or internal referencing may occur.

3.2.1 Psychological integrity

It is well established in the case law of the ECtHR that the notion of 'private life' covers the physical and psychological integrity of the person.[109] However, 'psychological integrity' has been scarcely addressed by the Court and remains largely undefined.[110] Certain aspects of individuals' mental self-determination are also protected by the freedoms of thought, religion, and opinion as their inner sides ('I

106 Merrills and Robertson, Human rights in Europe: A study of the European Convention on Human Rights (*e-book*), Section '*Freedom of correspondence*'.

107 *Golder v. the United Kingdom.*

108 *Klass and Others v. Germany*; *Big Brother Watch and Others v. the United Kingdom* (2021) [GC] App. No(s). 58170/13, 62322/14 & 24960/15 (ECtHR 25 May 2021)

109 *Niemietz v. Germany*; *Sentges v. the Netherlands*; *Pentiacova and Others v. Moldova*; *Tysiac v. Poland.*

110 Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Von Arnauld, Von Der Decken, and Susi (ed.), p. 388.

interna').[111] However, in matters unrelated to religion, the meaning has not been significantly discussed in relation to these rights.[112] Within the scope of Article 8 ECHR, the Court has considered negative effects on mental health and harms to reputation as intrusions to psychological integrity.[113]

However, the jurisprudence does not provide any guidance regarding whether mind interventions, such as manipulation of decision-making, fall within the concept of psychological integrity.[114] Physical integrity has been way more prominent in both case law and legal discourse, leaving the concept of psychological integrity without a clear definition. A possible explanation is the difficulty in restricting *how* someone is persuaded to have a particular opinion. Individuals influence each other's thoughts all the time. Unless such interventions are accompanied by intrusions to the physical integrity, they are typically not considered a legal issue.[115] For example, if psychiatric medication is administered without patient consent, this would typically be considered an intrusion to the individual's physical integrity rather than the psychological, although the drug alters how the patient thinks, feels, or behaves.[116]

Relating to psychological integrity, the psychological aspects of immersive technologies provide an important distinction between the Metaverse and internet-based platforms. The potential psychological effects of immersive technologies fundamentally transform the technology's impact on the users' privacy.[117] The immersion itself means that users feel like they are in a completely different environment, i.e., an

111 Article 9 and 10 ECHR.

112 Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Von Arnauld, Von Der Decken, and Susi (ed.), p. 389.

113 *Bensaid v. the United Kingdom*; *Kyriakides v. Cyprus* (2008) App. No. 39058/05 (ECtHR 16 October 2008); *Axel Springer AG v. Germany*, para 83

114 Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Von Arnauld, Von Der Decken, and Susi (ed.), p. 397.

115 Ibid., p. 390-91

116 See e.g., *X v. Finland* (2012) ECHR 2012, para 212.

117 Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', p. 19.

alternative reality. AR and VR experiences generate stimulation patterns for the user, such as light photons for the eyes, acoustic input for the ears, and tactile or haptic stimulators for touch.[118] The immersive experience is so convincing that brain activity, as measured by MRIs, shows responses in the hippocampus when a user experiences a virtual event that is akin to how the brain responds to an actual event.[119] In practical terms, immersive technologies are immensely persuasive to the point where discerning between an actual event and a virtual one becomes nearly impossible, at least on a psychological level. Despite *knowing* that the virtual event is not real, our brain's response fails to differentiate between the two realms.

To this background, immersive technologies combined with AI can potentially manipulate people's opinions in unprecedented ways. The actor who controls the immersive environment can determine the information individuals receive and influence the direction of one's opinions. Even if the intended message is resisted, AI solutions can analyze the biological reactions gathered through immersive technologies and adapt the stimuli to sway individuals' opinions towards a specific viewpoint. It's not unimaginable that this manipulation of opinions could be bought and sold to the highest bidder, putting not only privacy but democracy as a whole at risk.

Consequently, immersive experiences are psychologically different from interactions on internet-based platforms in that they provide incomparable methods to access and affect the human brain and mind. To this, it should be considered that the transition into various Metaverse applications is primarily led by a younger generation, who may possess a greater susceptibility to manipulation and a reduced inclination for critical thinking.[120] As put by Bublitz, "*the greater the extent to which the skull as the natural barrier of the mind becomes permeable, the more pressing the need to*

---

118 Strickland, Jonathan, 'How Virtual Reality Gear Works', *HowStuffWorks*. https://electronics.howstuffworks.com/gadgets/other-gadgets/VR-gear.htmpt6. (Accessed 2023-03-10).

119 Brown, Thackery I et al. 'Prospective representation of navigational goals in the human hippocampus'. *Science.* Vol. 352, No. 6291. 2016, 1323-26.

120 Garon, 'Legal implications of a ubiquitous metaverse and a Web3 future', p. 166 f.

draw normative limits to interventions".[121] Thus, I believe that the implementation of immersive technologies into several aspects of our lives calls for an interpretation of the right to psychological integrity that recognizes the human mind as an entity deserving the same level of human rights protection as our physical bodies.

Such an interpretation comes with challenges, particularly in terms of scope. What should be considered an intrusion to our psychological integrity, and what is simply a part of the mental effects we are exposed to as part of our life? Every change of opinion or negative impact on one's mental state cannot be considered an intrusion to psychological integrity. Bublitz argues that the scope must be limited so that only abnormal attacks on the mind qualifies as an intrusion.[122] On a practical level, a right to psychological integrity ought to manifest as a claim against others to abstain from interfering with one's mind. Assuming that to be the case, determining what an 'abnormal attack' is will ultimately be a question of the means used for interference. Using Metaverse technologies to manipulate an individual's thoughts and emotions differs fundamentally from traditional 'analog' methods in several aspects.

Firstly, novel technologies have the potential to penetrate and alter the mind of an individual on a far deeper level than analog methods, as they allow for a more precise and targeted manipulation of cognitive and affective processes.[123] Furthermore, the unknown objective behind these technologies means that they might operate covertly, making it difficult for the individual to detect or defend against the manipulation. Analog methods are typically more transparent in who the sender is, allowing individuals to identify the objective behind the communicated message and potentially resist the manipulation.

---

121 Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Von Arnauld, Von Der Decken, and Susi (ed.), p. 390.

122 Ibid., p. 400.

123 Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', p. 23 ff.

Suppose the right to psychological integrity in the Metaverse context is conceptualized as a claim to non-interference. In that case, it also means that right holders have the liberty to freely change their minds.[124] Such a liberty is not only a likely consequence of the non-interference, but also a natural limitation to the concept of psychological integrity. It would restrict the use of technology to manipulate an individual's thoughts and emotions while balancing opposing interests, such as the ability to freely debate issues and attempt to persuade people of one's conviction.

The interpretation of psychological integrity, as presented in this section, requires a thoughtful assessment of the potential risks involved and how they weigh against other rights and freedoms. The arguments presented in this section require further examination. However, the widespread use of Metaverse technologies will expose the human brain to unprecedented levels of large-scale and individualized manipulation, which justifies an increased focus on psychological integrity from a human rights perspective.

3.2.2 Data protection

The right to the protection of personal data is not an autonomous right in the ECHR. Instead, the Court has acknowledged that the protection of personal data is of fundamental importance to a person's enjoyment of their right to respect for private and family life, home, and correspondence, as guaranteed by Article 8 of the Convention.[125] The EctHR's case law regarding data protection covers an extensive realm of activities. As mentioned in the delimitations for this thesis, all of these are neither relevant in this context, nor possible to explore in depth given the time constraints of this project. Thus, two main aspects deemed relevant for the thesis topic will be explored further in depth, without making any claims to be an exhaustive examination of how data protection can be affected by Metaverse technologies.

---

[124] Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Von Arnauld, Von Der Decken, and Susi (ed.), p. 400.

[125] *Z v. Finland*; *M.K. v. France*; *S and Marper v. the United Kingdom*; *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland.*

3.2.2.1 Personal data as the basis for data protection

It is a fundamental notion that data protection mechanisms apply to personal data. The Court has defined 'personal data' with reference to Convention no. 108 for the protection of individuals with regard to automatic processing of personal data (Convention 108), where it is defined as "*any information relating to an identified or identifiable individual*".[126] This includes information that directly identifies an individual, such as names, and any elements that could indirectly identify an individual, such as IP addresses.[127] This definition is also in accordance with how personal data is defined in EU legislation, i.e., the GDPR.[128] Given that the rights and freedoms in the Convention are provided to individuals by the contracting states, it is intuitive that data protection, within the scope of private life, only applies to data relating to an individual.[129] This is also the case in many data protection and privacy laws worldwide. If data is aggregated, anonymized or deidentified, it does not fall within the scope of such laws.[130]

The implementation of Metaverse technologies challenges the notion that only data relating to an individual is worthy of protection. Many immersive technologies include facial recognition, emotion detection, and behavioral monitoring. These technologies can identify bodily traits and characteristics without necessarily identifying the person as a specific individual.[131] Combining such technologies with big data analytics and AI make it possible to affect individuals' lives and behavior without

---

126 Article 1 and 2 Convention no. 108 for the protection of individuals with regard to automatic processing of personal data (Convention 108); *Amann v. Switzerland* (2000) ECHR 2000-II, para 65; *Haralambie v. Romania* (2009) App. No. 21737/03 (ECtHR 27 October 2009), para 77.

127 E.g., *Garnaga v. Ukraine* (2013) App. No. 20390/07 (ECtHR 16 May 2013), para 36; *Benedik v. Slovenia* (2018) App. No. 62357/14 (ECtHR 24 April 2018), para 107-08.

128 Article 4 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 (General Data Protection Regulation) (GDPR).

129 See the phrasing in Article 1 ECHR.

130 Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, p. 115

131 Ricanek, K. and Barbour, B. 'What Are Soft Biometrics and How Can They Be Used?'. *Computer*. Vol. 44, No. 9. 2011, 106-08

directly identifying them.[132] Even when the data used *is* personal data, individuals are granted little control and oversight over how their personal data is used to draw inferences about them.[133] When the data is aggregated or anonymized, it is largely unregulated and falls outside the scope of data protection legislation and human rights frameworks.[134] This allows governments and companies to freely collect and process such data as they wish.

As these technologies improve, it is becoming easier to infer the identity of an individual by combining the anonymized data with other datasets that are often publicly available. Data anonymously collected in public spaces through IoT devices, and therefore not subject to data protection mechanisms, could be combined with datasets stemming from Metaverse interactions, making it possible for governments and companies to identify the individual retrospectively. Further, many wearable devices do not only affect the wearer. Often, wearables involve 'alwayson' audio and video recording technologies used to mirror places and environments that the wearer is in. The devices collect data from the wearer, but also capture pictures, movements, voices, and conversations of unknowing individuals who interact with the wearer in both the virtual and physical world.[135] These individuals are often unaware of this data collection and cannot opt-out. Since the collected 'bystander data' likely does not qualify as personal, the data collection is more or less unregulated. All this data could be combined with other data sets, allowing for identification.

When personal data is the basis for whether data protection mechanisms apply, it is very hard for individuals to have any control of the data that is collected in the former stage. The increasing complexity of data flows between different entities,

---

132 Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, p. 114-15.

133 Wachter, Sandra and Mittelstadt, Brent. 'A right to reasonable inferences: re-thinking data protection law in the age of big data and AI'. *Colum. Bus. L. Rev.* 2019, 494.

134 Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, p. 116.

135 Rodriguez, Katitza and Opsahl, Kurt, 'Augmented Reality Must Have Augmented Privacy', *The Electronic Frontier Foundation (EFF)*. 2020-10-16. https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy. (Accessed 2023-03-14).

which are often unknown to the individual, makes it challenging even to know who has access to data sets that could contain one's personal data. In principle, this could be solved in two ways; either, all data will ultimately be considered personal data due to the ever-decreasing possibility of effectively anonymizing data. Or, the criteria for when data is subject to data protection regulation can no longer be whether data is 'personal'.

None of these options are unproblematic. If all data is considered personal, the concept risks being diluted, along with its associated rights. Suppose another criterion is employed to qualify data as subject to data protection. In that case, it must be considered what such a criterion should look like and how it could be effectively implemented. Further, it is not apparent that the situations described above should be managed within the existing framework for data protection of personal data. It could be more suitable to construct alternative data protection frameworks that do not revolve around the notion of personal data but are designed to manage these technological challenges. That will not be further analyzed in this thesis.

Instead, this section concludes by stating that when more data is collected without our knowledge or control, the division between personal and non-personal data becomes increasingly complex. As described at the beginning of this section, data protection within the human rights realm is of fundamental importance to a person's enjoyment of their right to respect for private life. The current distinction between personal and non-personal data opens the door to actions that may de facto affect an individual's privacy. Still, it remains unregulated due to the data not being personal. Moving forward, this will require consideration to maintain the efficiency of data protection frameworks, especially from a human rights perspective.

3.2.2.2 Biometric data & AI

It has been held throughout this thesis that Metaverse technologies are likely to extensively increase and fundamentally change the character of the data collection that is carried out on a regular basis. Immersive technologies mainly depend on hardware to get information. The hardware records the user's body movements and functions, such as head nodding, blinking, and hand, feet, and finger movements.

Further, it records the user's emotional or physical states by measuring the activity in the brain using EEG, which records electrical activity in different parts of the brain, and EMG, which tracks signals that activate muscles.[136]

In this vein, it is relevant to analyze how current rules regarding biometric data apply to this kind of data collection. Article 6 of Convention 108 declares that biometric data uniquely identifying a person cannot be automatically processed unless domestic law provides appropriate safeguards. The Court has designated information falling within Article 6 of Convention 108 as 'sensitive' and warranting heightened protection.[137] The ECtHR has not provided a single definition of biometric data. However, in its case law, the Court has generally referred to biometric data as unique personal data that can be used for identification purposes, such as DNA profiles, fingerprints, and voice samples.[138] To offer a more general definition, Convention 108 defines biometric data as "*data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual*".[139] The Court has emphasized that authorities cannot use modern scientific techniques such as fingerprinting, collecting biological samples, and DNA profiling of people suspected or convicted of crimes without carefully considering the balance between the potential benefits and their privacy rights.[140] Further, the rapid pace of developments in the field of genetics and information technology implies that the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner that cannot be anticipated today.[141]

---

136 Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', p. 24.

137 European Court of Human Rights, *Guide to the Case-Law of the of the European Court of Human Rights - Data protection*, p. 11. 2022. https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf (Accessed 2023-05-15).

138 *Gaughran v. the United Kingdom* (2020) Application No. 45245/15 (ECtHR 13 February 2020); *S and Marper v. the United Kingdom*; *Van der Velden v. the Netherlands* (2006) ECHR 2006-XV; *Allan v. the United Kingdom* (2002) ECHR 2002-IX.

139 Article 6(58) Convention 108.

140 *S and Marper v. the United Kingdom*, para 112.

141 Ibid., para 71.

Two primary reflections can be made in relation to biometric data in the Metaverse context. First, the definition of biometric data must be considered. As no single definition is offered in the Court's case law, the notion of biometric data remains open to final interpretation. However, it's clear that legal definitions of biometric data generally are related to identification.[142] This limitation could present a gap in the definition of biometric data. If physiological data is used to determine a person's likes, interests, or motivations instead of their identity, it most likely does not qualify as biometric data.[143] The extensive capabilities of immersive environments offer numerous possibilities for collecting and utilizing this information in unprecedented ways.

Even when accounting for the identification criteria, it should be considered how combinations of data sets that separately do not qualify as biometric data, but that in combination could, are to be treated. The combination of a user's head tilt while in a VR headset and records of their gestures in an immersive environment can be equally identifying as their fingerprint or retinas.[144] 'Multimodal' biometric databases are further of interest, where multiple biometrics are collected and stored in one database.[145] In the database, the biometrics are combined with conventional data such as name, address, social security number, gender, and race. Geolocation tracking technologies are then put on top of the datasets, which could enable constant surveillance.[146] This might call for a more pragmatic and dynamic definition of biometric data. How, and for what purpose, data sets are combined should be considered when determining if particular data is worthy of the extended data protection mechanisms applied to sensitive data.

---

142 See e.g., Article 6(58) Convention 108; Article 4(14) GDPR; Section 1798.140 (b) California Consumer Privacy Act of 2018 (CCPA).

143 Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', p. 37.

144 Ibid., p. 36.

145 'Biometrics', *The Electronic Frontier Foundation (EFF)*. https://www.eff.org/issues/biometrics. (Accessed 2023-03-15)

146 Ibid.

Second, under current conditions, biometric data is generally collected under extraordinary circumstances, often in a criminal law enforcement context. Metaverse technologies are likely to change this. Immersive technologies must collect biometric data to function.[147] The collection of biometric data will no longer be contained in the relatively controlled environment of law enforcement. Instead, it will be carried out in an automatic, casual manner that is unpreceded by a balance of interests. This data can be used for, e.g., remote biometric identification, emotion recognition, and biometric categorization.[148] This has been pointed out as "*a particular intrusiveness upon the right to privacy and the dignity of individuals, coupled with a special risk of adverse impact on other human rights and fundamental freedoms*" by the Consultative Committee of Convention 108.[149] The risks related to biometric data are also highlighted in the proposed AI Act, which bans remote biometric identification in public places in real-time and retrospectively.[150]

To this background, it should be considered how biometric data can be collected, stored, and processed. The ECtHR has underlined that state legislation must guarantee that the processing of biometric data is effectively protected from abuse and emphasized the need for safeguards when automatic processing is deployed.[151] Storing biometric data related to non-convicted people for unlimited periods of time in a nationwide database processed by automated means for criminal-identification purposes has been considered a violation of Article 8.[152] The Court stated that such 'blanket and indiscriminate' retention of fingerprints, cellular samples, and DNA

147 Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', p. 27.

148 Fuster, Gloria González and Peeters, Michalina Nadolna. 'Person identification, human rights and ethical principles - Rethinking biometrics in the era of artificial intelligence'. *Panel for the Future of Science and Technology*. 2021.

149 The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Facial Recognition*, 2021. (T-PD(2020)03rev4). https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (Accessed 2023-03-14).

150 Article 5 of the Proposal for the Artificial Intelligence Act (COM/2021/206 final) (AI Act).

151 *S and Marper v. the United Kingdom*, para 103.

152 Ibid., para 77 and 86.

profiles does not "*strike a fair balance between the competing public and private interests*" and was considered a disproportionate interference with the right to respect for private life.[153] Further, the Court has emphasized the significance of continuously improving technological capacities when assessing violations of Article 8 ECHR. For example, when an individual's photograph was held on a local database that did not have facial recognition or facial mapping software, the assessment concerning Article 8 should be based on the fact that these photographs *could* be uploaded to a national database with such software.[154]

The Court articulated the above principles in *S and Marper v. UK* and *Gaughran v. UK*. If a 'blanket and indiscriminate' retention of biometric data for criminal-identification purposes is considered a violation of Article 8, the mass collection of biometric data outside the criminal law context ought to be problematic. By definition, the technologies used to build the Metaverse require the mass collection of biometric data of both users and bystanders. Given the wide array of Metaverse applications and interoperability between the platforms, such data will be stored and processed by both private and public actors. For such data collection to strike a fair balance between the competing public and private interests, the meaning of 'public interest' must be reevaluated, as the power balance and the *modus operandi* are fundamentally different from the law enforcement context that the case law relating to biometric data predominantly has focused on.

In *S and Marper v. UK*, the respondent state argued that the "*detection and prosecution of serious crime and by exculpating the innocent*" were in the public interest.[155] Similar arguments were used in *Gaughran v. UK*, highlighting the difficulties in applying the public interest criteria outside the context of criminal law enforcement.[156]

153 Ibid., para 125.

154 *Gaughran v. the United Kingdom*, para 69 and 86.

155 *S and Marper v. the United Kingdom*, para 24.

156 *Gaughran v. the United Kingdom*, para 93

The collection of biometric data from nearly all individuals, without assessing and balancing public and private interests, can hardly be deemed proportionate. In *Gaughran v. UK*, the respondent state justified the interference by stating that fingerprint and DNA samples could only be identified by experts or with sophisticated equipment, and the stored material represents objective identifying material that can only be relevant or of use when compared with comparative material taken from a person lawfully subjected to a requirement to provide such material for comparison.[157]

However, with the emergence of Metaverse technologies, such equipment will be more widely available, and biometric data will be collected on a large scale regardless of legal obligations to provide it. The collection of biometric data in public spaces is arguably on such a high level that it is not deemed personal data and, as such, is not covered by data protection of human rights frameworks. This issue is discussed in Section 3.2.2.1 above. In private relationships, data collection is typically based on the data subject's consent.[158] However, such consent is often provided without a complete understanding of the implications. As Elizabeth Renieris has pointed out, we could "*individually consent our way into the same kind of surveillance state emerging in authoritarian regions of the world, especially in light of qualitatively different emerging technologies*".[159] Consequently, it is necessary to evaluate the circumstances, and especially the public interest criteria, relating to collecting biometric data in the Metaverse context, where the safeguards associated with law enforcement are absent.

3.2.3 Physical spaces

While being used to construct virtual worlds, the implementation of Metaverse technologies does not leave the physical spaces of the real world unaffected. The physical space that an individual is in has implications on how the right to privacy is interpreted. For example, certain aspects of the right to privacy apply only when the

[157] Ibid., para 11.

[158] See e.g., Article 9(1) GDPR.

[159] Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, p. 111.

individual is within the physical boundaries of their home.[160] In other cases, the Court has held that there can be a zone of interaction between a person with others, even in a public context, which may fall within the scope of 'private life.'[161] This section analyzes how aspects that revolve around a physical space, such as an individual's home and places that are considered 'public,' are affected by the implementation of Metaverse technologies.

3.2.3.1 Home

In the phrasing of Article 8 ECHR, an individual's home is explicitly included as a concept deserving of protection. Specifically, police entry, searches, and seizures in an individual's home are considered interferences with the right to respect for one's home.[162] Metaverse technologies can potentially lead to authorities having access to personal information about an individual's home without physically accessing it. When using immersive technologies in your home, AR and VR devices create a highly accurate digital representation of your space. By using audio and video recordings of the inside of your house and putting that data through simultaneous localization and mapping systems, a detailed map of your home can be created, including exact details, such as the location of items such as a mug on a coffee table.[163]

This allows authorities to investigate details of one's home that would previously have been impossible without physical intrusion. Thus, to ensure that the right to respect for one's home is upheld in the Metaverse era, the notion of 'home' might require a more extensive interpretation which includes digital representations of one's personal space. Further, what constitutes a 'search' of someone's home ought to include what some scholars refer to as 'virtual searches', i.e., investigatory techniques carried out covertly, remotely, and technologically rather than through physical in-

160 *Dragan Petrović v. Serbia* (2020) App. No. 75229/10 (ECtHR 12 April 2020), para 74.

161 *Von Hannover v. Germany* (no. 2) (2012) ECHR 2012, para 95.

162 *Gutsanovi v. Bulgaria*; *Buck v. Germany*; *Funke v. France*.

163 Opsahl, Kurt, 'Come Back with a Warrant for my Virtual House', *The Electronic Frontier Foundation (EFF)*. 2020-10-05. https://www.eff.org/deeplinks/2020/10/come-back-warrant-my-virtual-house. (Accessed 2023-03-14).

trusion.[164] This would ensure that digital searches of an individual's home are subject to the same proportionality test as physical ones, namely that it must be in accordance with the law, serve a legitimate aim and be necessary in a democratic society.[165]

3.2.3.2 Public spaces

Metaverse technologies are not confined to affecting how our homes can be monitored, but also how public spaces can be monitored. AR technologies blend physical and virtual worlds. When people use these technologies in public spaces – a current, real-life example being Pokémon Go – they record the surroundings, and more importantly, the people in the surroundings. As the technologies increase in sophistication, so do the surveillance opportunities. If someone is wearing augmented reality glasses, they may be able to record their conversations and create a detailed, real-time map of their surroundings. This might happen with or without the knowledge of the wearer. If these technologies become sufficiently widespread, it enables constant surveillance on a global scale, where individuals are continuously monitored in public or semi-public areas.[166]

Further, the interdependency between IoT devices and the Metaverse is notable in this context. Building the IoT entails embedding sensors, cameras, software, and an internet connection in everyday objects such as streetlights or trashcans. This facilitates exact data collection about what is happening in that city.[167] While this data could be used beneficially, such as for reducing traffic or improving infrastructure, it also includes detailed information about the behavior of everyone within the

---

164 Slobogin, Christopher. *Virtual Searches: Regulating the Covert World of Technological Policing.* New York, USA: New York University Press (2022) p. viii f.

165 Article 8(2) ECHR.

166 Rodriguez, Katitza and Mir, Rory, 'If Privacy Dies in VR, It Dies in Real Life', *The Electronic Frontier Foundation (EFF).* 2020-08-25. https://www.eff.org/deeplinks/2020/08/if-privacy-dies-vr-it-dies-real-life. (Accessed 2023-03-15).

167 Green, *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*, p. 92.

city.[168] While this data collection may be on such a high level that it does not relate to identifiable individuals, the combination of data sets described in *Section 3.2.2.2* has to be considered. Combined with the highly personal data collected by Metaverse technologies, allowing for identification based on body language, facial recognition, or even eye movements, the data collected by IoT devices in public spaces facilitates unprecedented opportunities for governments and companies to surveil entire communities without offering any proportionality assessment in each specific case. The initial phases of this type of monitoring are already evident. Notable instances of its implementation are the identification of people involved in the demonstrations after George Floyd's death in May 2020 and the US Capitol attack in January 2021.[169] Previously, law enforcement agencies have depended on official government sources like mugshots, driver's licenses, and passport photos to create image databases, but are increasingly turning to other sources of facial imagery that are publicly available or acquired from private entities.[170] Metaverse and IoT technologies are a goldmine for conducting this type of surveillance and building these databases.

Several rulings from the ECtHR touch upon the limits of monitoring individuals in public spaces. In *P.G. and J.H. v. UK*, which concerned voice surveillance at a police station, the Court reiterated that there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life.'[171] The ECtHR noted as follows.

> *A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent*

168 Ibid.

169 Slobogin, Christopher and Brayne, Sarah. 'Surveillance Technologies and Constitutional Law'. *Annual Review of Criminology.* Vol. 6, No. 1. 2023, 219-40, p. 222 f.

170 Ibid.

171 *P.G. and J.H. v. the United Kingdom* (2001) ECHR 2001-IX, para 56; *Von Hannover v. Germany* (no. 2), para 95.

record comes into existence of such material from the public domain.[172]

The Court elaborated on the issue in *Peck v. UK*, where it found that the monitoring of the actions of an individual in a public place by the use of photographic equipment, which does not record the visual data, does not per se give rise to an interference with the individual's private life.[173] Conversely, there might be interference with individuals' private life if the data recording is of a systematic or permanent nature.[174] To this background, it is questionable if the systematic data collection that occurs through widespread implementation of Metaverse and IoT technologies can be compatible with respect for private life as warranted by Article 8 ECHR.

Building on *Peck v. UK* and *P.G. and J.H. v. UK*, the core question in the assessment ought to be whether the data collection is 'of a systematic or permanent nature.' When assessing this, the Court has primarily focused on whether the data collection is permanently recorded, in the sense that the data is retained after the initial collection.[175] As the data gathered through Metaverse technologies is not only stored, but also processed, shared, and analyzed, the data collection ought to be considered as of a systematic or permanent nature. Further, the Court's case law states that how certain data might be used in light of the rapid pace of technological developments can be "*legitimate and relevant to a determination of the issue of whether there has been an interference*".[176]

This means that the potential for future surveillance using data collected by Metaverse and IoT technologies in public spaces could be considered when determining whether or not such data collection constitutes a violation of the right to privacy. Given the emerging character of these technologies and the difficulty in predicting how they will evolve, this is of elevated importance. The scale of adoption of

---

172 *P.G. and J.H. v. the United Kingdom*, para 57.

173 *Peck v. the United Kingdom* (2003) ECHR 2003-I, para 59.

174 Fuster and Peeters, 'Person identification, human rights and ethical principles - Rethinking biometrics in the era of artificial intelligence', p. 31.

175 *P.G. and J.H. v. the United Kingdom*, para 57-58; *Peck v. the United Kingdom*, para 59-60.

176 *S and Marper v. the United Kingdom*, para 71.

these technologies is closely connected to their intrusiveness. As more people use these devices, the surveillance possibility increases. The higher the ability to combine data sets from public and private settings, e.g., to identify people, the more intrusive the surveillance. Therefore, the legality of this data collection should, to the extent it is possible, be assessed with careful consideration of the potential for future surveillance rather than the current.

3.3 Concluding remarks

In conclusion, the emergence of Metaverse technologies is expected to significantly impact the right to privacy, primarily due to the exponential increase in the amount of data, both in width and depth, collected about individuals on a daily basis. The internet was the last technology to bring about such a shift, prompting a change in our conventional understanding of privacy concerning our bodies, homes, and correspondence. This change subsequently led to the implementation of initial national laws on data protection.[177] This section has argued that Metaverse technologies are likely to impact privacy in similar ways, including issues related to psychological integrity, biometric data collection, and surveillance of physical spaces. While these technologies offer numerous benefits, they also pose new challenges that must be addressed. As we move forward into the Metaverse era, it will be crucial to balance the benefits of these technologies with the protection of individual privacy rights, ensuring that the right to privacy remains protected in the digital realm.

[177] Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, p. 34.

4 Jurisdiction in the Metaverse

In this chapter, virtual human rights infringements in the Metaverse context, along with their jurisdictional impact, are explored and exemplified. The case law relating to the concept of jurisdiction is summarized, and the models employed by the ECtHR are presented, applied, and analyzed in the Metaverse context to assess their suitability for virtual human rights infringements. Lastly, alternative models for defining jurisdiction, stemming from academic literature and case law, are presented and analyzed.

4.1 Jurisdictional issues in the Metaverse

The Metaverse is a rapidly evolving digital space that could give rise to significant jurisdictional challenges. The issues that arise can be complex, as virtual worlds often transcend national borders and involve multiple legal systems.[178] The jurisdictional issues of the Metaverse were displayed in the case of *Bragg v. Linden Research, Inc.*, where the U.S. District Court for the Eastern District of Pennsylvania was faced with determining whether it had jurisdiction over a dispute involving virtual property in the virtual world *Second Life*. Because the parties were located in different states, and the virtual property had a monetary value, the court found that it had jurisdiction over the dispute.[179]

In principle, jurisdiction refers to the authority to enforce a body of law and the means to do so.[180] The concept of jurisdiction is commonly linked to the notion of territory, but it is also recognized to exist separately or beyond territorial limitations.[181] In relation to human rights, and particularly the applicability of the ECHR, this implies that the human rights outlined in the Convention generally apply to sub-

---

178 Kalyvaki, 'Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction'.

179 *Bragg v. Linden Research, Inc.* (2007) 487 F. Supp. 2d 593 (E.D. Pa).

180 Dorsett, Shaunnagh and McVeigh, Shaun. *Jurisdiction*. London: Routledge (2012) p. 4 ff.

181 Singh, 'Criminal Jurisdiction in the Metaverse'.

jects located within the territorial boundaries of a contracting state. However, as jurisdiction can be considered to exist separately and beyond territorial limitations, there are situations in which the rights and freedoms of the Convention can and should apply outside said territorial boundaries.[182] With the Metaverse having a global reach, situations where jurisdictional issues str central in determining the practical application of human rights frameworks are likely to occur, as exemplified below. In each example, the actions are assumed to represent a violation of the relevant right or freedom, without conducting an in-depth analysis of the substantive aspects.

Consider that Person A, located in Country A, uses a virtual assistant in the Metaverse that collects their highly sensitive personal data. The virtual assistant is owned by a company in Country B. Person A's data is shared with the government of Country B as part of their surveillance program, infringing Person A's right to privacy. The violation is carried out by Country B in their territory. Whether Person A is considered within the jurisdiction of Country B, despite being located outside their territorial borders, will determine whether their right to privacy is protected in this situation.

Another example is that Person A, located in Country A, and Person B, located in Country B, meet on a Metaverse platform which is owned and operated by a company in Country B, where state control over private companies is apparent. Person A tells Person B that s/he is a member of a particular political party and is planning to host a virtual demonstration relating to a certain social issue. Because such demonstrations are illegal in Person B's country, s/he reports Person A to the authorities. Country B suspends Person A's account and shuts down the virtual demonstration, violating Person A's freedom of expression. Once again, Country B violates Person A's rights remotely, rendering the question of jurisdiction the determining factor in whether Person A enjoys the protection of the ECHR in the given situation.

[182] Besson, Samantha. 'The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to'. *Leiden Journal of International Law*. Vol. 25, No. 4. 2012, 857-84.

These two examples are relatively intuitive, as jurisdictional issues relating to privacy and freedom of expression have also been present in the current digital world.[183] While Metaverse technologies are expected to elevate the scope and effect of these issues, they could also give rise to jurisdictional issues regarding other human rights, which are more novel in the context of virtual human rights infringements.

First, immersive technologies have the potential to extend the application of rights that were previously limited to physical environments and primarily corporeal experiences. For example, the prohibition of torture enshrined in Article 3 ECHR could be enacted in virtual settings thanks to immersive technologies. For example, instead of putting an individual in prison, it would be possible to place a criminal in a virtual environment that mimics already established physical environments used for punishment.[184] It has been proposed that VR could be used to decrease overcrowding in prisons by making house arrest a realistic option for nonviolent offenders. A VR system could monitor the individual's activity, and the person could remain under house arrest instead of being incarcerated if they complete a certain amount of monitored VR hours. The VR system would then include features that make the house arrest more prison-like, such as creating a sense of solitude at home, or including rehabilitation activities such as VR education courses.[185]

This places immense power in the hands of the person or institution in control of the VR system. It also opens up new opportunities for virtual human rights infringements. What happens, for example, if the controller of the VR system decides to amplify the punishment by placing the prisoner in a virtual environment where

---

183 See e.g., Aswad, Evelyn Mary. 'The future of freedom of expression online'. *Duke L. & Tech. Rev.* Vol. 17. 2018, 26; Reidenberg, Joel R. 'Technology and Internet Jurisdiction'. *University of Pennsylvania Law Review.* Vol. 153, No. 6. 2005, 1951-74; Svantesson, Dan Jerker B. Solving the Internet Jurisdiction Puzzle. *Oxford University Press* (2017).

184 The technology to do this has already existed for some years, and is developing continuously, see e.g., Davies, Caroline, 'Welcome to your virtual cell: could you survive solitary confinement?', *The Guardian*, 2016; Gash, Tom, 'Forget prisons, the future of punishment will be virtual', *Wired*, 2020.

185 Greenbaum, Dov. 'VR in the Prison System: Ethical and Legal Concerns'. *AJOB Neuroscience.* Vol. 13, No. 3. 2022, 158-60.

she is in solitary confinement? Or, force the prisoner to listen to heavy-metal music playing at a high volume throughout the monitored VR hours? Or, if the criminal fears spiders, he is placed in a virtual prison with one spider crawling around his cell. Every day, an additional spider is added to his jail cell, until eventually, there would be hundreds of spiders. As the spiders crawl on him, he feels the experience through his haptic sense.[186] Numerous examples similar to these could be envisioned, but the key point remains: the capabilities of virtual imprisonment and virtual punishment make it imperative to consider their potential implications for, e.g., the prohibition of torture. These actions are carried out remotely, and such punishments could easily be executed across state borders. Extradition of prisoners would no longer be necessary. 'Enhanced interrogation' similar to that carried out by the CIA on Al-Qaeda detainees after 9/11 could be performed without state agents traveling to the foreign black sites where detainees are held.[187] This puts the most fundamental provisions of the ECHR into play with regard to virtual human rights infringements and makes the jurisdictional issue essential.

Finally, the Metaverse is expected to create a virtual financial ecosystem similar to the real world, transferring parts of people's private economies to this virtual space. This creates technical uncertainty surrounding, e.g., the seizure of virtual property. A state that controls platform, cloud, or server providers could seize virtual property belonging to individuals located abroad. This could result in substantial financial losses for those affected. Moreover, this could violate individuals' property rights under Protocol 1 of the ECHR. As with the other examples, this violation occurs remotely with the victim located outside the jurisdiction of the respondent state. In light of these examples, exploring how the jurisdiction criteria in the ECHR can be understood in a virtual context is relevant.

---

186 These examples are derived from Moncada, Jose A. 'Virtual reality as punishment'. *Indiana Journal of Law and Social Equality*. Vol. 8. 2020, 304, p. 319 ff.

187 The ECtHR have decided several cases regarding human rights abuses in the CIA 'black sites' in Poland, but from the perspective of the territorial state, rather than the state that directly committed the abuse, see Milanovic, Marko, 'Extraterritoriality and human rights: prospects and challenges', in Thomas Gammeltoft-Hansen and Jens Vedsted-Hansen (eds.), *Human Rights and the Dark Side of Globalisation* (London: Routledge, 2016) 67-92. See specifically Footnote 13 and the therein cited case law.

4.2 The 'jurisdiction' criteria

To determine whether individuals outside the territory of a contracting state are entitled to the protection of the ECHR, it is necessary to examine the jurisdiction criteria in Article 1 ECHR in more detail. Article 1 ECHR states that:

> *The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.*

Consequently, jurisdiction is a prerequisite for a state party to be held accountable for a human rights violation.[188] To this, it should be noted that an individual is not required to be a citizen of a contracting state to be considered within that state's jurisdiction.[189] In reverse, the mere fact that an individual is a citizen of a contracting state does not automatically place her within that state's jurisdiction.[190] Following the textual meaning of the word, jurisdiction primarily refers to a state's territory.[191] However, several cases exist where states have been held accountable for acts committed in the territories of other states. The ECtHR has stated that extraterritorial jurisdiction can be established according to the personal and spatial models.[192] Most cases where these models have been tried regard various forms of military operations and state forces acting outside the territorial scope of the state.[193]

---

188 *Ilaşcu and Others v. Moldova and Russia* (2004) ECHR 2004-VII, para 311.

189 Lemmens, Koen, 'General Survey of the Convention', in P Van Dijck et al. (eds.), *Theory and Practice of the European Convention on Human Rights* (Intersentia, 2018) 1-78, p. 11.

190 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 99.

191 *Banković and Others v. Belgium* (2001) ECHR 2001-XII, para 61, 66 and 67. See also Cameron, *An introduction to the European Convention on Human Rights*, p. 54.

192 *Cyprus v. Turkey* (1975) (dec.) D.R. 2, p. 125; *Loizidou v. Turkey* (1995) (preliminary objections) [GC] Series A No. 310; Milanovic, Marko. *Extraterritorial application of human rights treaties: law, principles, and policy.* Oxford University Press (2011) p. 118.

193 See e.g., the cited case-law in European Court of Human Rights, *Guide on Article 1 of the European Convention on Human Rights: Obligation to respect human rights – Concepts of "jurisdiction" and imputability*, 2022. https://www.echr.coe.int/documents/guide_art_1_eng.pdf (Accessed 2023-02-28).

To this date, the ECtHR has not addressed the jurisdiction criteria in any case where technology has facilitated human rights violations of individuals outside the state's territory.[194] Noteworthy is that the Court could have addressed this on several occasions, e.g., in *Big Brother Watch v. UK*, *Liberty v. UK*, and *Weber v. Germany*.[195] Each of these cases concerned infringements to Article 8 and 10 of the ECHR, which were carried out virtually and outside the territorial borders of the respondent state. However, in all these cases, the Court has either avoided the issue altogether and dismissed the case as ill-founded on the merits or assumed that the jurisdictional criterion was fulfilled.[196] To this background, it is relevant to analyze how the models for determining jurisdiction apply to virtual human rights infringements, which are progressively facilitated by Metaverse technologies.

4.3 Models for defining jurisdiction

The ECtHR has established that a state can be considered to exercise jurisdiction outside its border according to the personal and spatial models. The background and essence of each model are summarized in the following sections. Then, each model is applied and analyzed in relation to the examples set out above.

4.3.1 The personal model

The personal model entails that extraterritorial jurisdiction can be established based on the power or control exercised over the *person* of the applicant.[197] Firstly, it should be noted that for the personal model to apply, exceptional circumstances regarding the nature of the connection between the applicant and the respondent state must exist. The fact that decisions taken at the national level impacted the

194 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 92.

195 *Big Brother Watch and Others v. the United Kingdom*; *Liberty and Others v. the United Kingdom* (2008) App. No. 58243/00 (ECtHR 1 July 2008); *Weber and Saravia v. Germany* (2006) (dec.) ECHR 2006-XI.

196 Lubin, Asaf. 'Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)'. *International Legal Materials*. Vol. 61, No. 4. 2022, 605-53.

197 Milanovic, *Extraterritorial application of human rights treaties: law, principles, and policy*, p. 118.

situation of persons abroad is insufficient to establish extraterritorial jurisdiction.[198] The model was first set out in *Cyprus v. Turkey* in 1975.[199] In subsequent cases, the ECtHR demonstrated reluctance to define jurisdiction based on control over an individual. In *Banković v. Belgium*, the Court argued that the drafters had not intended for the ECHR to apply that extensively.[200] However, the ECtHR has subsequently confirmed the personal model. In *Issa v. Turkey*, the Court stated that a state could be held accountable for violations of the Convention concerning victims located in the territory of another state, if the victims are under the former state's authority and control through its agents operating - lawfully or unlawfully - in the latter state. The reasoning behind this was that Article 1 ECHR could not be interpreted in a manner that allows violations on the territory of another state, which the state party could not perpetrate on its territory.[201]

The personal model was further elaborated in *Al-Skeini v. UK*, destined to replace the criticized ruling in *Banković v. Belgium* as the leading extraterritorial case of the ECtHR.[202] In *Al-Skeini v. UK*, the personal model was summarized to apply in three distinct situations; (1) the acts of diplomatic and consular agents, (2) the exercise of extra-territorial public powers with the consent, at the invitation or with the acquiescence of the foreign government concerned or, (3) the use of force by state agents extra-territorially to bring an individual under their control.[203]

According to *Al-Skeini v. UK*, the personal model's determining factor is whether the state exercises authority and control over the individual.[204] This means that, in theory, the personal model could apply in situations where both the individual

198 *M.N. and Others v. Belgium* (2020) (dec.) App. No. 3599/18 (ECtHR 5 May 2020), para 112.

199 *Cyprus v. Turkey*, para 8.

200 *Banković and Others v. Belgium*, para 75.

201 *Issa and Others v. Turkey* (2005) App. No. 31821/96 (ECtHR 16 November 2004), para 71.

202 Milanovic, Marko. 'Al-Skeini and Al-Jedda in Strasbourg'. *European Journal of International Law*. Vol. 23, No. 1. 2012, 121-39, p. 121-22.

203 *Al-Skeini and Others v. the United Kingdom* (2011) [GC] ECHR 2011, para 131 ff.

204 Ibid., para 136-37.

and the interference with their rights occurs outside the state's territory - if the state still is considered to exercise authority and control over the individual through the actions which constitute a virtual violation of their human rights. The obvious question is, therefore, what qualifies as 'authority or control' and how these criteria would apply to virtual human rights violations.

The majority of the Court's case law where the personal model has been applied involves the exercise of physical custody.[205] Inherently, cases of virtual human rights infringements typically do not include elements of physical custody. Virtual human rights violations would be prohibited if conducted by Country A against an individual located within the territorial borders of Country A. The motives behind the personal model state that the Convention cannot be interpreted so that it allows violations on the territory of another state, which the state party could not perpetrate on its territory.[206] This would seem to indicate that a virtual human rights violation cannot be allowed when carried out by Country A against an individual located in Country B, as that would indeed allow Country A to commit an infringement on the territory of Country B that they could not perpetrate on their territory. This sparks the question of whether virtual violations can qualify as an exercise of authority and control despite the absence of physical elements.

There are several cases where the personal model has been applied despite the absence of physical custody.[207] While the detailed circumstances naturally differ, the individuals in all these cases were shot from a distance, without being within the territorial borders or in the custody of the respondent state. In *Al-Skeini v. UK*, the

---

205 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 100; See also *Öcalan v. Turkey* (2005) ECHR 2005-IV; *Ramirez Sanchez v. France* (2006) ECHR 2006-IX; *Al-Saadoon and Mufdhi v. the United Kingdom* (2010) ECHR 2010; *Al-Jedda v. the United Kingdom* (2011) ECHR 2011; *Maria Isaak and Others v. Turkey* (2006) (dec.) App. No. 44587/98 (ECtHR 28 September 2006).

206 *Issa and Others v. Turkey*, para 71.

207 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 100; See also *Pad and Others v. Turkey* (2007) (dec.) App. No. 60167/00 (ECtHR 28 June 2007); *Al-Skeini and Others v. the United Kingdom*; *Jaloud v. the Netherlands* (2014) ECHR 2014.

personal model was applied to the killings of the applicants. However, the victims were also present in an area where the UK exercised public powers usually exercised by Iraq's government, which was highly relevant. If the UK had not exercised such public powers, the personal model of jurisdiction would not have applied.[208] This indicates that the capacity to kill is 'authority and control' over the individual when combined with public powers. Still, the killing does not in itself amount to 'authority and control' when elements of physical custody are absent.[209] It has been argued that the inclusion of 'public powers' as a prerequisite for applying the personal model is an effort to prop up its viability and prevent its potential collapse, i.e., that it results in the unrestricted application of the ECHR.[210] Regardless of whether such an attempt to tailor the circumstances to create a viable model actually occurred, the mixture of circumstances that amounted to jurisdiction in *Al-Skeini v. UK* leaves the definition of 'authority and control' in the absence of physical custody unclear.[211]

In the subsequent case of *Jaloud v. the Netherlands*, the victim was shot from a distance when passing through an Iraq checkpoint controlled by Dutch troops. The Dutch troops were considered to exercise 'authority and control over persons passing through the checkpoint' given that they controlled the victim's right to life at that time.[212] Therefore, the ECtHR concluded that the Netherlands had jurisdiction. This was found in the absence of physical control over the victim, effective control over the area, and the exercise of public powers. This could imply that the ECtHR is shifting towards an approach where jurisdiction is based on the exercise of authority and control over an individual's *rights* rather than an individual's *person*.[213]

---

208 Milanovic, 'Al-Skeini and Al-Jedda in Strasbourg', p. 130.

209 *Al-Skeini and Others v. the United Kingdom*, para 143-48; Milanovic, 'Al-Skeini and Al-Jedda in Strasbourg', p. 130.

210 Milanovic, 'Extraterritoriality and human rights: prospects and challenges', in Gammeltoft-Hansen and Vedsted-Hansen (ed.).

211 Milanovic, 'Al-Skeini and Al-Jedda in Strasbourg', p. 131.

212 *Jaloud v. the Netherlands*, para 152.

213 Watt, 'The role of international human rights law in the protection of online privacy in the age of surveillance', p. 10.

This would indicate that if a state controls the victim's rights, jurisdiction based on the personal model can exist in cases of virtual human rights violations. However, such an interpretation must be made with caution. Otherwise, the consequence could be what Watt refers to as a 'cause and effect' notion of jurisdiction, i.e., if a state *can* violate a person's rights, that automatically amounts to jurisdiction.[214] Such an interpretation could erode the jurisdictional threshold. It should be noted that Jaloud v. the Netherlands, similar to Al-Skeini v. UK, includes a combination of several factors to establish jurisdiction, where each isolated factor would likely not have sufficed to establish jurisdiction.[215] Thus, it remains unclear if the control over a victim's human rights at a particular time, isolated from surrounding factors, amounts to jurisdiction.

It is also evident that the application of the personal model without physical custody has been limited to severe circumstances where the absolute rights of the Conventions, particularly the right to life, have been jeopardized. These cases must be viewed in the context that they involve the most fundamental provisions in the Convention.[216] Failure to establish jurisdiction in these cases would create a precedent that contradicts the very basis of the Convention. Virtual violations have typically concerned other rights, such as privacy and freedom of expression. This indicates that an analogous application of *Jaloud v. the Netherlands* to virtual human rights violations might be inappropriate. However, as exemplified in *Section 4.1*, virtual human rights infringements fueled by Metaverse technologies could indeed affect the absolute rights in the Convention, e.g., the prohibition of torture, which speaks to the suitability of applying the reasoning in *Jaloud v. the Netherlands* to such cases.

---

214 Watt, 'The role of international human rights law in the protection of online privacy in the age of surveillance', p. 10 f.; see also Haijer, Friederycke and Ryngaert, Cedric. 'Reflections on Jaloud v. the Netherlands: jurisdictional consequences and resonance in Dutch society'. *Journal of International Peacekeeping*. Vol. 19, No. 1-2. 2015, 174-89, p. 180.

215 Sari, Aurel. 'Untangling Extra-Territorial Jurisdiction from International Responsibility in Jaloud v. Netherlands: Old Problem, New Solutions'. *Military Law and Law of War Review*. Vol. 53, No. 2. 2014, 287-318, p. 299 ff.

216 See e.g., *Giuliani and Gaggio v. Italy* (2011) [GC] ECHR 2011 (extracts), para 174, regarding that Article 2 and 3 are considered the most fundamental provisions in the Convention.

Accordingly, it remains debatable whether adapted versions of the personal model are suitable for managing virtual human rights violations. As the Court intended, the model is adequate to analyze actions conducted abroad by state officials or their alleged agents. However, the emphasis on physical control over persons does not translate well into the virtual domain.[217] As argued by Milanovic, an attempt to do so risks leading to the personal model collapsing into the universal application of the Convention.[218] This is similar to the 'cause and effect' notion of jurisdiction discussed above. Conclusively, the application of the personal model to virtual human rights violations is fraught with difficulties, the most significant of which is the risk of either being too restrictive and thereby endangering the effective protection of human rights, or being too permissive, thereby reducing the practical meaning of the jurisdictional threshold and allowing for automatic jurisdiction based on the ability to carry out a human rights violation.

4.3.2 The spatial model

The spatial model entails that extraterritorial jurisdiction can be established based on the control exercised over the foreign *territory* in question.[219] The spatial model is generally considered less controversial than the personal model.[220] The ECtHR first articulated the spatial model in *Loizidou v. Turkey*, where it established that jurisdiction in cases of military occupation of a territory should be based on actual, effective control over the territory.[221] It does not matter if such control was obtained lawfully or unlawfully. All cases where the spatial model has been applied include control over foreign territory in the context of an armed conflict.[222] The 'effective

---

217 Watt, 'The role of international human rights law in the protection of online privacy in the age of surveillance', p. 10; Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism', p. 2150.

218 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 129.

219 Milanovic, *Extraterritorial application of human rights treaties: law, principles, and policy*, p. 118.

220 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 112.

221 *Loizidou v. Turkey*, para 62.

222 *Guide on Article 1 of the European Convention on Human Rights: Obligation to respect human rights – Concepts of "jurisdiction" and imputability*, p. 24.

overall control test' proposed in *Loizidou v. Turkey* is viable and relatively clear.[223] However, Milanovic argues that such clarity comes at a price, since there are many situations where a state is capable of violating the rights of individuals without controlling the actual area, rendering the spatial model too limiting.[224]

The spatial model will apply if the individual is outside the territorial boundaries of the respondent state, but is located in an area occupied and effectively controlled by the respondent state.[225] In such situations, the state is obliged to ensure the individual's human rights under Article 1.[226] However, situations matching the above circumstances are intrinsically far from the virtual human rights violations that are likely to occur in the Metaverse context. As demonstrated by the examples described in Section 4.1, virtual human rights violations occur when technology enables violations to occur without physical proximity between the individual, the respondent state, and the violation. In the Metaverse, individuals from different parts of the world come together to interact, information and data are transmitted globally in real-time, and companies in various states provide platforms, technologies, and hardware. As a result, determining jurisdiction in such cases can be exceedingly complex.

It is evident that a state can infringe on an individual's human rights without the individual being physically present. For example, a privacy violation could physically occur in a particular state – say, in Sweden – and have extraterritorial effects upon individuals across the globe. For example, suppose that vast amounts of sensitive personal data are collected from people worldwide and stored on servers in Sweden. If the Swedish government unlawfully processes that data, it could violate the right to privacy of the data subjects, who are located in multiple contracting states to the ECHR. This sparks the question of whether the location of the individual or the location of the violation is the basis for the area subject to the 'effective over-

223 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 122 f.

224 Ibid., p. 124 f.

225 *Loizidou v. Turkey*, para 62.

226 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 122 f.

all control test.'[227] If the individual's physical location is decisive in determining jurisdiction, all individuals outside of Sweden are not under Sweden's jurisdiction as per the ECHR. If the location of the violation is decisive, all victims are under Sweden's jurisdiction. Milanovic clarifies this, stating that the inquiry is whether the individual is considered under the state's jurisdiction. 'Jurisdiction' under the spatial model means an area under the state's effective control. Thus, the location of the violation must be considered irrelevant.[228] Therefore, it ought to be difficult, if not completely contrary to the textual and conceptual definition of the spatial model, to successfully argue that the model can be applied based on the location of the violation.

To conclude, applying the spatial model to virtual human rights infringements occurring in the Metaverse context could often generate a problematic outcome where the individual's rights are endangered, because the focus of the model is on the location of the individual rather than the location of the violation. This allows states to commit virtual human rights infringements and use a 'jurisdiction'-based defense, relieving them of their responsibility as long as they refrain from engaging in such violations against individuals within their territory. States may avoid the jurisdiction of the ECHR by only violating the rights of individuals in other states. This could lead to what is often referred to as 'collusion for circumvention'.[229] By working together, states can conduct surveillance or confiscate virtual property from their citizens engaged in undesirable activities, as long as they do so outside their jurisdiction but on behalf of the state where the individual is located. Although this may sound overly conspiratorial, the data-sharing practices of the 'Five Eyes' alliance and the Europe Pact demonstrate that such situations can and do occur.[230] It should be noted that the arguments presented here do not assert that such practices

227 Ibid., p. 124 f.

228 Ibid.

229 Watt, 'The role of international human rights law in the protection of online privacy in the age of surveillance', p. 11.

230 See e.g., 'Mass surveillance - Which countries could have access to your data?', *Amnesty International UK*. 2015. https://www.amnesty.org.uk/which-countries-access-your-data-nsa-gchq-five-eyes-snowden-surveillance. (Accessed 2023-03-05).

are inherently unlawful in all circumstances, as that is not always the case. However, if these situations do not meet the jurisdictional threshold for applying the ECHR, such practices would not need to be justified in relation to the relevant human rights provision to be deemed lawful. From a human rights perspective, this would leave the situation largely uncontrolled, with potentially harmful consequences. To this background, exploring how alternative approaches for defining jurisdiction hold up in a virtual context is warranted.

4.4 Alternative approaches for defining jurisdiction

As accounted for above, the personal and spatial models are inadequate when dealing with virtual human rights infringements. The emergence of the Metaverse means that the opportunities for virtual human rights infringements increase and migrate to other rights than privacy. Therefore, this section will analyze and apply three alternative approaches for defining jurisdiction in cases of virtual human rights infringements. These approaches have been derived from Eliza Watt's article *The role of international human rights law in the protection of online privacy in the age of surveillance* and Holly Huxtable's article *E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance.*

Initially, two of the models have been proposed in legal doctrine as a response to the Edward Snowden revelations, where it became evident that new technologies could facilitate virtual human rights violations, particularly concerning the right to privacy. The last approach analyzed in this thesis was proposed by Judge Bonello in his concurring opinion in *Al-Skeini v. UK*, and does not explicitly relate to virtual human rights infringements, but is aimed at managing extraterritorial human rights violations in general. Each of the approaches is well-cited and highly relevant to the topic. Thus, they offer a suitable starting point for examining alternative ways of managing jurisdictional issues in the Metaverse era.

4.4.1 The 'third' approach - based on positive vs. negative obligations

Milanovic suggests a 'third' approach, which differentiates between the positive obligation of states to guarantee human rights, which includes preventing violations by third parties, and the negative obligations, which includes refraining from infringing upon individuals' rights without proper justification.[231] The textual phrasing of Article 1 ECHR holds that states are to *secure* the rights and freedoms to everyone within their jurisdiction. It does not explicitly state that states have a negative obligation to *respect* the rights and freedoms of the Convention.[232] However, the Court has generally assumed that negative obligations are inherent in the Convention.[233]

According to this approach, the term 'jurisdiction' would mainly refer to having effective control over a territory, and the positive responsibility to protect human rights would be linked to a state's ability to exert such control over the area. This is because, in most cases, a state would require such control to fulfill its positive obligation to protect human rights. On the other hand, the negative obligation to refrain from violating human rights would apply without territorial limits or any jurisdiction threshold.[234] The logic behind not limiting the negative obligation is that, contrary to positive obligations, it is always possible for states to comply with them as they are in complete control of their own state organs.

The 'third model' entails that the ECHR would apply to virtual human rights violations, given that they either (1) are executed within the territorial borders of the contracting state, or (2) falls within the negative obligations of the contracting state. In other words, if a virtual human rights infringement is carried out within the territory of the contracting state, the state has both positive and negative obligations under the ECHR. Suppose the virtual human rights infringement is instead

---

231 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 118-19.

232 Compared to e.g., Article 2(1) of the ICCPR which states that "Each State Party to the present Covenant undertakes to *respect* and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant" (emphasis added).

233 Shelton, Dinah and Gould, Ariel, 'Positive and Negative Obligations', in Dinah Shelton (ed.), *The Oxford Handbook of International Human Rights Law* (Oxford University Press, 2013) p. 569-70.

234 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 119.

extraterritorial. In that case, the state only has negative obligations, i.e., it is only responsible if the violation is directly attributable to the state party rather than private corporations residing in that country.

While this distinction may seem clear-cut, it cannot be assumed to be so in practice. Positive and negative obligations are often closely interconnected. Situations could arise where states are in a position to stop third parties from committing human rights abuses even without territorial control. Under the 'third' approach, their obligations would not extend to such situations.[235] This is especially relevant in the digital context, where private companies often wield immense power over human rights infringements. The prevailing view is that corporations do not have human rights obligations under the law. The state has this obligation, meaning it has a legal duty to prevent corporate abuse. In practice, states must implement regulatory and legislative frameworks to ensure that private corporations act in a manner that respects human rights and are held accountable in instances in which they fail.[236]

To exemplify that the state's obligation could be too narrow, consider the following. Meta's (formerly Facebook) European HQ is located in Ireland.[237] Under the 'third' approach, Ireland's positive obligation to protect human rights would be contained to their territory. As Meta must abide by Irish legislation, Ireland ought to have a stronger position than other countries to enact legislation that protects the right to privacy even in the private relationship between Meta and their users, inside and outside Ireland's territorial borders. On the contrary, it could be argued that firms which operate in multiple states are generally subject to the laws and regulations of each country where they conduct business, rather than just the laws of the country

235 da Costa, Karen. 'Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy'. *Human Rights Law Review*. Vol. 13, No. 2. 2013, 417-20.

236 Callamard, Agnès, 'The Human Rights Obligations of Non-State Actors', in Rikke Frank Jørgensen (ed.), *Human Rights in the Age of Platforms* (Cambridge, Massachusetts: The MIT Press, 2019) p. 201 ff.

237 Meta, 'Facebook to Establish International Headquarters in Dublin, Ireland'. Press release 2008-10-02. https://about.fb.com/news/2008/10/facebook-to-establish-international-headquarters-in-dublin-ireland/.

where they are registered.[238] While this is true, it should be considered that it is common that the question of which country's laws apply ultimately is decided contractually. Continuing with the example of Meta, their Terms of Service state that any dispute must be resolved in a competent court in Ireland, and Irish law will apply to such claim or dispute without regard to conflict of law provisions.[239] As this applies regardless of the counterparty's location, it places Ireland in a better position than other countries to enact legislation that protects human rights in the private relationship between Meta and their users. As Jon Garon puts it, "*the ToS* [terms of service] *for a universal platform has the potential to become the equivalent of positive national law*".[240] If that is the case, only the existing national law has the authority to decide the legality of such terms of service. This implies that states do not always require territorial control to fulfill their positive obligation to protect human rights.

The situation is, however, complex. Following Milanovic's reasoning that states require territorial control to fulfill their positive obligation, it might be equally unreasonable to extend Ireland's positive obligations outside their territorial borders for the sole purpose that a company is registered in that country. In conclusion, while Milanovic's model does promote the universal protection of human rights, the distinction between positive and negative obligations as the determining factor might not consider all perspectives of virtual human rights violations. Nonetheless, the difficulty in developing such an all-encompassing model must be acknowledged. While it might not live up to that exceptionally high standard, the 'third' approach does, as stated by Milanovic himself, have the advantage of being clear and predictable, precluding many arbitrary outcomes, and providing a relatively stable balance between considerations of universality and effectiveness.[241]

---

238 See e.g., Ruggie, John Gerard. 'Business and human rights: the evolving international agenda'. *American Journal of International Law*. Vol. 101, No. 4. 2007, 819-40.

239 Meta, *Terms of Service*, Section 4.4. 2023. https://www.facebook.com/legal/terms (Accessed 2023-04-26).

240 Garon, 'Legal implications of a ubiquitous metaverse and a Web3 future', p. 208.

241 Milanovic, 'Human rights treaties and foreign surveillance: Privacy in the digital age', p. 119.

4.4.2 The virtual approach - based on control of rights

The virtual approach is introduced by Margulies and encompasses that jurisdiction should be determined based on a 'virtual control' test. The practical implication would be that the ECHR applies when a state can assert 'virtual control' over an individual's rights,[242] even though it lacks control over the territory or the 'person' of the individual.[243] The virtual model has faced criticism for being a novel concept that lacks support from shared legal expectations about jurisdiction.[244] Nevertheless, as Watt points out, the model has several advantages.[245] Firstly, it aligns with the notion of control that the ECtHR recognizes. Secondly, it addresses the jurisdictional complexities of human rights obligations in virtual cases, as governments can control an individual's rights at the click of a button. Thirdly, it is consistent with the ECtHR's reasoning in *Jaloud v. the Netherlands*, where a broader approach was adopted, and extraterritorial jurisdiction was established based on the exercise of authority and control over the individual's right to life, rendering physical proximity irrelevant.[246]

However, the application of the virtual model could give rise to issues. As previously discussed concerning *Jaloud v. the Netherlands*, this approach could entail a 'cause and effect' notion of jurisdiction, i.e., if a state *can* violate a person's rights, it automatically amounts to jurisdiction. If that were sufficient, the jurisdiction criterion would practically not apply to cases of virtual human rights violations, as the occurrence of the violation would be determining jurisdiction, rather than jurisdiction being an independent prerequisite. Thus, it is difficult to determine the

---

242 Margulies uses the term 'communications' where I use the much broader term 'rights'. I do so because the Metaverse context, as opposed to current online platforms, can facilitate virtual infringements to other rights than privacy, which is the right primarily implied by the term 'communications'. See Section 4.1 for an elaborate discussion on this matter.

243 Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism', p. 2139.

244 See e.g., Paust, Jordan J. 'Can You Hear Me Now: Private Communication, National Security, and the Human Rights Disconnect'. *Chi. J. Int'l L.* Vol. 15. 2014, 612.

245 Watt, 'The role of international human rights law in the protection of online privacy in the age of surveillance', p. 12.

246 *Jaloud v. the Netherlands*, para 152.

delimitations of the model in a way that does not result in precisely the 'cause and effect' definition of jurisdiction that is arguably undesirable.[247]

4.4.3 The functional approach - based on principles of human rights law

The functional approach is based on the notion that the foundational principles of human rights law can inform interpretations of extraterritorial jurisdiction. Instead of deciding on extraterritorial jurisdiction on a case-by-case basis, jurisdiction under the functional model is established when a state takes any action outside its territory that would be prohibited on its territory.[248] This approach was used in the first cases involving the extraterritorial reach of the ICCPR, such as *Lopez Burgos v. Uruguay*, where it was deemed unacceptable to interpret a state's responsibility under Article 2 of the Covenant as allowing them to commit violations of the Covenant in another country that they could not execute on their territory.[249] This case subsequently inspired the expansion of the extraterritorial application of the ECHR.[250]

In relation to the ECHR, the functional model is commonly attributed to the separate opinion of Judge Bonello in *Al-Skeini v. UK*. Judge Bonello proposes a 'functional test' as the threshold for examining how foundational human rights principles should be interpreted in relation to extraterritorial human rights violations.[251] Under this test, a state is considered to exercise jurisdiction "*whenever it falls within its power to perform, or not to perform*" any of the five key functions ensuring the observance of human rights.[252] These key functions include (1) not violating (through their agents) human rights, (2) having in place systems that prevent breaches of human rights, (3) investigating complaints of human rights abuses, (4) scourging

247 See e.g., *Banković and Others v. Belgium*, para 75; Haijer and Ryngaert, 'Reflections on Jaloud v. the Netherlands: jurisdictional consequences and resonance in Dutch society', p. 180.

248 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 105.

249 *Sergio Euben Lopez-Burgos v. Uruguay* (1979) UN HR Committee, Communication No 52/1979.

250 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 105.

251 Ibid.

252 *Al-Skeini and Others v. the United Kingdom*, concurring opinion of Judge Bonello, para 11.

those of their agents who infringe human rights, and (5) compensating the victims of breaches of human rights.[253] According to Huxtable, one determining factor for jurisdiction under the functional model is whether it depended on the agents of the state if the alleged violation was committed. If yes, jurisdiction is established.[254]

Applying this test to a virtual human rights infringement, this question can be answered in the affirmative when the action is directly attributable to the state. The question of jurisdiction would consequently correspond to the question of attribution.[255] In light of this, the approach has been criticized for essentially amounting to the 'cause and effect' jurisdiction rejected in *Banković v. Belgium*.[256] The argument is that the model extends the scope of obligations so far that the centrality of state borders and the inherent fact that the purpose of jurisdiction is to limit state obligations are undermined.[257] Further, as discussed regarding the 'third' approach, using attribution as a delimitation for jurisdiction might be unsatisfactory given the high impact that private companies have on the facilitation and execution of virtual human rights infringements. Though, unlike Huxtable, I believe that the second key function presented by Judge Bonello, namely having in place systems that prevent breaches of human rights, could be interpreted as addressing this deficiency. If a state has the power to put systems in place that prevent human rights violations, they are considered to exercise jurisdiction.

---

253 Ibid., para 10.

254 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 108-09. The second factor put forward by Huxtable is whether it was within the power of the state to punish the perpetrators and to compensate the victims. Since the functions proposed by Judge Bonello are alternative and not cumulative, I have chosen not to discuss this issue in depth as I consider it to be of inferior relevance to the topic of this thesis.

255 Wide, 'Exporting Privacy - A Study on the Extraterritorial Application of the European Convention on Human Rights to Foreign Mass Surveillance', p 47.

256 Huxtable, 'E.T. Phoned Home... They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', p. 108 f.

257 Banković and Others v. Belgium, para 75; Ovey, Clare, 'ECHR in Armed Conflict', in Katja S Ziegler, Elizabeth Wicks, and Loveday Hodson (eds.), *The UK and European Human Rights: A Strained Relationship?* (Bloomsbury Publishing, 2015) p. 231.

To exemplify, let's revisit the example regarding Ireland's positive obligation to prevent human rights violations from private entities residing within their territorial borders, e.g., Meta. Under the functional model, any virtual human rights violation victim would be considered within the Irish jurisdiction, if Ireland has the power to enact systems to prevent said violation. This offers a broad application of the ECHR to virtual human rights violations, and, consequently, a high protection for individuals. However, the practical implications of this are problematic. It might be unreasonable to extend Ireland's positive obligations outside its territorial borders for the sole purpose that a company is registered in that country. While that country is in a better position than others to put systems in place that protect human rights, as private corporations must abide by the national legislation of that state, other practical implications must be considered. To give a hands-on example; if Ireland is responsible for all alleged virtual human rights infringements committed by Meta, the increased burden on the national Irish courts to administer these proceedings is a non-negligible argument for the inefficiency of such an interpretation of jurisdiction.

4.5 Concluding remarks

To conclude, the existing jurisdictional models need to be revised when it comes to addressing virtual privacy violations due to their inadequate adaptation to digital technologies that have become ubiquitous in modern times. These models were formulated by international human rights courts and organizations long before the rise of the Metaverse technologies, making them ill-suited to address the complexities of the virtual age. The current approaches that emphasize physical control over individuals or territory are inappropriate for online activities, let alone the Metaverse. The alternative approaches have all received some criticism. Most commonly, extending the jurisdiction criteria beyond control over territory or persons could lead to a 'cause and effect' definition of jurisdiction, which may be problematic, as it practically removes the jurisdictional threshold entirely.

This is a much bigger and more politically sensitive question than the interpretation of the jurisdictional threshold. Thus, I believe that models that claim to define jurisdiction but ultimately result in the removal of the jurisdictional threshold are inherently flawed. To this end, the 'third' approach offers the most transparent solu-

tion, as it clearly argues for removing the jurisdiction criteria for the negative obligations of the contracting states. This approach provides much-needed clarity, given that all the examined models, both current and alternative, suffer from arbitrary elements that complicate the determination of jurisdiction in cases of extraterritorial human rights infringements. By removing this ambiguity, the 'third' approach offers a clear and consistent solution that is welcome in this context. However, the distinct position that private companies have in the creation and operation of the digital landscape implies that the 'third' approach may be too limiting when precluding states from having positive obligations outside their territorial borders.

Leaving this issue unsolved allows states to exploit the gap in jurisdictional definitions and continue or increase their interference with a wide range of human rights. To prevent this, it is essential to recognize the fundamental differences between physical and virtual human rights violations and implement a more comprehensive approach to defining jurisdiction. This does not necessarily mean abandoning the personal and spatial model entirely, as they are well-motivated by legal certainty. I will conclude my analysis by stating that virtual human rights violations make it complex to define jurisdiction in a way that balances legal certainty with effective human rights protection.

One possible conclusion is that the digitalization of society represents such a fundamental change in the context that human rights operate in that jurisdiction is no longer an appropriate threshold. To state this with certainty, however, requires a more in-depth analysis than can be accommodated within this thesis's scope, which is not necessarily attainable given the uncertainty that characterizes technological disruption. Many perspectives – not least practical and political – require consideration. Therefore, there is a need for further research and discussion on developing a more appropriate jurisdictional model for virtual human rights violations in the age of the Metaverse.

5 Conclusion

In this chapter, the research questions are revisited, and a short conclusion for each question is presented.

Research Question 1: *How can the Metaverse and its associated technologies affect the interpretation of the right to privacy?*

The emergence of Metaverse technologies is expected to significantly impact various aspects of privacy, given the vast amount of information collected about individuals. These technologies provide governments and organizations with access to new information about individuals, challenging traditional notions of privacy. Three main observations need to be considered. Firstly, Metaverse technologies can collect significantly more detailed and broader information than what is currently possible with online platforms. Secondly, these technologies collect data not only about the individual user, but also about the people and spaces surrounding them. Lastly, combining this information with advanced AI systems can affect individuals' opinions and emotions at unprecedented levels. Based on these observations, this thesis concludes that Metaverse technologies raise concerns about psychological integrity, biometric data collection, and surveillance of physical spaces. While there may be other areas where the right to privacy could be affected by Metaverse technologies, these are the areas where the increased depth and breadth of data collection currently are expected to have the most significant impact.

Research Question 2: *How do current models for defining jurisdiction apply to virtual human rights infringements occurring outside the territorial borders of the respondent state?*

This thesis concludes that the current models for jurisdiction are insufficient for virtual human rights violations. They were created before the rise of digital technology and do not address the complexities of the virtual context. Both the spatial

and personal models emphasize physical control, which is challenging to apply in the Metaverse context and to online activities in general. Specifically, physical borders are not barriers to committing human rights violations when states can control the human rights of individuals outside their jurisdiction remotely. This allows states to evade their human rights obligations, as the jurisdictional threshold could prohibit the application of human rights treaties to virtual human rights violations. There is a need to adjust the models for defining jurisdiction to account for the characteristics of the virtual context.

Research Question 3: *How do alternative approaches for defining jurisdiction apply to virtual human rights infringements occurring outside the territorial borders of the respondent state, and do they contribute to protecting human rights in the Metaverse context?*

Considering the shortcomings of existing models for defining jurisdiction, alternative approaches have been proposed in academia and case law. The models investigated in this thesis are (1) the 'third' approach, which is based on positive/negative obligations, (2) the virtual approach, which is based on control of the human right at hand, and (3) the functional approach, which is based on key principles of human rights law. Despite these attempts, none of the proposed models for defining jurisdiction have been without criticism. The most commonly addressed issue is that the alternative approaches render the jurisdiction criterion completely insignificant, as the ability to commit a human rights violation automatically means that the violation was within the jurisdiction of the respondent state. Thus, the question of attribution will be identical to that of jurisdiction. Furthermore, creating another model for defining jurisdiction tailored to specific situations can lead to increased fragmentation and ambiguity in the case law. The emergence of virtual human rights violations has made it challenging to define jurisdiction in a way that balances legal certainty with effective human rights protection. Therefore, it may be necessary to reassess whether jurisdiction is an appropriate threshold for safeguarding human rights in a digitalized society. However, this topic requires further analysis beyond the scope of this thesis.

6 Discussion and further research

Throughout the work with this thesis, the complexity of predicting how emerging technologies will affect a particular legal area, and vice versa, has become clear to me. I have also encountered some reflections that I have chosen to omit from the academic analysis because they would extend the scope of this thesis to the extent that it was not manageable within the time frame. Such reflections are briefly discussed in the following, along with propositions for further research.

Throughout the work with this thesis, the complexity of predicting how emerging technologies will affect a particular legal area, and vice versa, has become clear to me. I have also encountered some reflections that I have chosen to omit from the academic analysis because they would extend the scope of this thesis to the extent that it was not manageable within the time frame. Such reflections are briefly discussed in the following, along with propositions for further research.

Further, the implications of blockchain technology in protecting the right to privacy is an exciting area that presents a more optimistic and solution-oriented approach to privacy concerns than the often pessimistic outlook surrounding the issue. With its decentralized and immutable characteristics, blockchain can provide users with greater control over their personal information, enabling them to choose what data to share and with whom. Decentralization also eliminates the need for intermediaries such as corporations, reducing the risk of data breaches and unauthorized access. If reaching widespread adoption, these two aspects could transform the entire data collection and privacy landscape, triggering a significant shift in how organizations approach the storage, management, and use of personal information. Exploring how this might affect privacy rights is an interesting topic for future research.

Bibliography

Legislation

California Consumer Privacy Act (CCPA), CA Civ Code § 1798.192 (2018).

Charter of Fundamental Rights of the European Union (2000/C 364/01).

Convention no. 108 for the protection of individuals with regard to automatic processing of personal data.

International Covenant on Civil and Political Rights.

Proposal for the Artificial Intelligence Act (COM/2021/206 final).

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 (General Data Protection Regulation).

The Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights).

Universal Declaration of Human Rights.

Cases

X. v. the Federal Republic of Germany (1970) No. 3603/68, Commission decision of 4 February 1970, Collection of Decisions, 31, pp. 48-50,
ECLI:CE:ECHR:1970:0204DEC000360368

Golder v. the United Kingdom (1975) Series A No. 18,
ECLI:CE:ECHR:1975:0221JUD000445170

Cyprus v. Turkey (1975) (dec.) D.R. 2, p. 125,
ECLI:CE:ECHR:1975:0526DEC000678074

Klass and Others v. Germany (1978) Series A No. 28,
ECLI:CE:ECHR:1978:0906JUD000502971

Sergio Euben Lopez-Burgos v. Uruguay (1979) UN HR Committee,
Communication No 52/1979, UN Doc CCPR/C/13/D/52/1979

Marckx v. Belgium (1979) Series A, No. 31.,
ECLI:CE:ECHR:1979:0613JUD000683374

Abdulaziz, Cabales and Balkandali v. UK (1985) Series A No. 94,
ECLI:CE:ECHR:1985:0528JUD000921480

Johnston and Others v. Ireland (1986) Series A No. 112,
ECLI:CE:ECHR:1986:1218JUD000969782

Niemietz v. Germany (1992) Series A No. 251-B,
ECLI:CE:ECHR:1992:1216JUD001371088

Lüdi v. Switzerland (1992) Series A No. 238.,
ECLI:CE:ECHR:1992:0615JUD001243386

Funke v. France (1993) Series A No. 256-A,
ECLI:CE:ECHR:1993:0225JUD001082884

Burghartz v. Switzerland (1994) Series A No. 280-B,
ECLI:CE:ECHR:1994:0222JUD001621390

Loizidou v. Turkey (1995) (preliminary objections) [GC] Series A No. 310,
ECLI:CE:ECHR:1995:0323JUD001531889

M.S v. Sweden (1997) Reports of Judgments and Decisions 1997-IV,
ECLI:CE:ECHR:1997:0827JUD002083792

Z v. Finland (1997) Reports of Judgments and Decisions 1997-I,
ECLI:CE:ECHR:1997:0225JUD002200993

Amann v. Switzerland (2000) ECHR 2000-II,
ECLI:CE:ECHR:2000:0216JUD002779895

P.G. and J.H. v. the United Kingdom (2001) ECHR 2001-IX,
ECLI:CE:ECHR:2001:0925JUD004478798

Bensaid v. the United Kingdom (2001) ECHR 2001-I,
ECLI:CE:ECHR:2001:0206JUD004459998

Banković and Others v. Belgium (2001) ECHR 2001-XII,
ECLI:CE:ECHR:2001:1212DEC005220799

Al-Adsani v. the United Kingdom (2001) ECHR 2001-XI,
ECLI:CE:ECHR:2001:1121JUD003576397

Allan v. the United Kingdom (2002) ECHR 2002-IX,
ECLI:CE:ECHR:2002:1105JUD004853999

Peck v. the United Kingdom (2003) ECHR 2003-I,
ECLI:CE:ECHR:2003:0128JUD004464798

Sentges v. the Netherlands (2004) App No. 27677/02 (ECtHR 8 July 2003),
ECLI:CE:ECHR:2003:0708DEC002767702

Ilaşcu and Others v. Moldova and Russia (2004) ECHR 2004-VII,
ECLI:CE:ECHR:2004:0708JUD004878799

M.K. v. France (2005) App. No. 19522/09 (ECtHR 18 April 2013),
ECLI:CE:ECHR:2013:0418JUD001952209

Issa and Others v. Turkey (2005) App. No. 31821/96 (ECtHR 16 November 2004),
ECLI:CE:ECHR:2004:1116JUD003182196

Öcalan v. Turkey (2005) ECHR 2005-IV,
ECLI:CE:ECHR:2005:0512JUD004622199

Buck v. Germany (2005) ECHR 2005-IV,
ECLI:CE:ECHR:2005:0428JUD004160498

Pentiacova and Others v. Moldova (2005) ECHR 2005-I,
ECLI:CE:ECHR:2005:0104DEC001446203

Ramirez Sanchez v. France (2006) ECHR 2006-IX,
ECLI:CE:ECHR:2006:0704JUD005945000

Van der Velden v. the Netherlands (2006) ECHR 2006-XV,
ECLI:CE:ECHR:2006:1207DEC002951405

Maria Isaak and Others v. Turkey (2006) (dec.) App. No. 44587/98 (ECtHR 28 September 2006), ECLI:CE:ECHR:2006:0928DEC004458798

Weber and Saravia v. Germany (2006) (dec.) ECHR 2006-XI,
ECLI:CE:ECHR:2006:0629DEC005493400

Pad and Others v. Turkey (2007) (dec.) App. No. 60167/00 (ECtHR 28 June 2007),
ECLI:CE:ECHR:2007:0628DEC006016700

Tysiac v. Poland (2007) ECHR 2007-I,
ECLI:CE:ECHR:2007:0320JUD000541003

Bragg v. Linden Research, Inc. (2007) 487 F. Supp. 2d 593 (E.D. Pa)

S and Marper v. the United Kingdom (2008) ECHR 2008,
ECLI:CE:ECHR:2008:1204JUD003056204

Liberty and Others v. the United Kingdom (2008) App. No. 58243/00 (ECtHR 1 July 2008), ECLI:CE:ECHR:2008:0701JUD005824300

Kyriakides v. Cyprus (2008) App. No. 39058/05 (ECtHR 16 October 2008),
ECLI:CE:ECHR:2008:1016JUD003905805

Haralambie v. Romania (2009) App. No. 21737/03 (ECtHR 27 October 2009), ECLI:CE:ECHR:2009:1027JUD002173703

Al-Saadoon and Mufdhi v. the United Kingdom (2010) ECHR 2010, ECLI:CE:ECHR:2010:0302JUD006149808

Al-Skeini and Others v. the United Kingdom (2011) [GC] ECHR 2011, ECLI:CE:ECHR:2011:0707JUD005572107

Al-Jedda v. the United Kingdom (2011) ECHR 2011, ECLI:CE:ECHR:2011:0707JUD002702108

Giuliani and Gaggio v. Italy (2011) [GC] ECHR 2011 (extracts), ECLI:CE:ECHR:2011:0324JUD002345802

X v. Finland (2012) ECHR 2012, ECLI:CE:ECHR:2012:0703JUD003480604

Von Hannover v. Germany (no. 2) (2012) ECHR 2012, ECLI:CE:ECHR:2012:0207JUD004066008

Axel Springer AG v. Germany (2012) [GC] App. No. 39954/08 (ECtHR 7 February 2012), ECLI:CE:ECHR:2012:0207JUD003995408

Winterstein and Others v. France, (2013) App. No. 27013/07 (ECtHR 17 October 2013), ECLI:CE:ECHR:2013:1017JUD002701307

Garnaga v. Ukraine (2013) App. No. 20390/07 (ECtHR 16 May 2013), ECLI:CE:ECHR:2013:0516JUD002039007

Gutsanovi v. Bulgaria (2013) ECHR 2013 (extracts), ECLI:CE:ECHR:2013:1015JUD003452910

Jaloud v. the Netherlands (2014) ECHR 2014, ECLI:CE:ECHR:2014:1120JUD004770808

Chiragov and Others v. Armenia (2015) [GC] ECHR 2015, ECLI:CE:ECHR:2015:0616JUD001321605

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (2017) ECHR 2017 (extracts), ECLI:CE:ECHR:2017:0627JUD000093113

Denisov v. Ukraine (2018) [GC] App. No. 76639/11 (ECtHR 25 September 2018), ECLI:CE:ECHR:2018:0925JUD007663911

Naït-Liman v. Switzerland (2018) [GC] ECHR 2018, ECLI:CE:ECHR:2018:0315JUD005135707

Benedik v. Slovenia (2018) App. No. 62357/14 (ECtHR 24 April 2018), ECLI:CE:ECHR:2018:0424JUD006235714

Gaughran v. the United Kingdom (2020) Application No. 45245/15 (ECtHR 13 February 2020), ECLI:CE:ECHR:2020:0213JUD004524515

Dragan Petrović v. Serbia (2020) App. No. 75229/10 (ECtHR 12 April 2020), ECLI:CE:ECHR:2020:0414JUD007522910

M.N. and Others v. Belgium (2020) (dec.) App. No. 3599/18 (ECtHR 5 May 2020), ECLI:CE:ECHR:2020:0505DEC000359918

Big Brother Watch and Others v. the United Kingdom (2021) [GC] App. No(s). 58170/13, 62322/14 & 24960/15 (ECtHR 25 May 2021), ECLI:CE:ECHR:2021:0525JUD005817013

Books

Ball, Matthew, *The Metaverse: And How It Will Revolutionize Everything*. 1st edn. New York: Liveright Publishing Corporation, a division of W.W. Norton Company. 2022.

Bates, Ed, *The evolution of the European Convention on Human Rights: from its inception to the creation of a permanent Court of Human Rights.* Oxford University Press. 2010.

Cameron, Iain, *An introduction to the European Convention on Human Rights*. 8th edn. Uppsala: Iustus. 2018.

Dorsett, Shaunnagh and McVeigh, Shaun, *Jurisdiction*. London: Routledge. 2012.

Green, Ben, *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. Ideas Series. Cambridge: The MIT Press. 2019.

Holtzman, David H, *Privacy lost: how technology is endangering your privacy*. John Wiley & Sons. 2006.

Milanovic, Marko, *Extraterritorial application of human rights treaties: law, principles, and policy*. Oxford University Press. 2011.

Renieris, Elizabeth M, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*. MIT Press. 2023.

Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare: ämne, material, metod, argumentation och språk*. 5th edn. Stockholm: Norstedts Juridik. 2021.

Slobogin, Christopher, *Virtual Searches: Regulating the Covert World of Technological Policing*. New York, USA: New York University Press. 2022.

Stephenson, Neal, *Snow crash: A novel*. Spectra. 2003.

Svantesson, Dan Jerker B, *Solving the Internet Jurisdiction Puzzle*. Oxford University Press. 2017.

E-books

Merrills, J. G. and Robertson, A. H., Human rights in Europe: A study of the European Convention on Human Rights *(e-book)*. 4th edn. Manchester: Manchester University Press. 2022. https://www.perlego.com/book/3805430/human-rights-in-europe-a-study-of-the-european-convention-on-human-rights-pdf

Book sections

Bublitz, Jan-Christoph, 'The Nascent Right to Psychological Integrity and Mental Self-Determination', in Andreas von Arnauld, Kerstin von der Decken, and Mart Susi (eds.), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (Cambridge: Cambridge University Press), 387-403. 2020.

Callamard, Agnès, 'The Human Rights Obligations of Non-State Actors', in Rikke Frank Jørgensen (ed.), *Human Rights in the Age of Platforms* (Cambridge, Massachusetts: The MIT Press). 2019.

Gräns, Minna, 'Allmänt om användningen av andra vetenskaper inom juridiken', in Maria Nääv and Mauro Zamboni (eds.), *Juridisk metodlära* (2nd edn.; Lund: Studentlitteratur), 429-42. 2018.

Hyun-joo, Jeon, et al., 'Blockchain and AI Meet in the Metaverse', in M. Fernández-Caramés Tiago and Fraga-Lamas Paula (eds.), *Advances in the Convergence of Blockchain and Artificial Intelligence* (Rijeka: IntechOpen), Ch. 5. 2021.

Kindt, Els J., 'The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing', in Pompeu Casanovas and Giovanni Sartor (eds.), *Privacy and Data Protection Issues of Biometric Applications - Part of the Law, Governance and Technology Series book series* (Dordrecht: Springer Netherlands), 403-567. 2013.

Kleineman, Jan, 'Rättsdogmatisk metod', in Maria Nääv and Mauro Zamboni (eds.), *Juridisk metodlära* (2nd edn.; Lund: Studentlitteratur), 21-47. 2018.

Lemmens, Koen, 'General Survey of the Convention', in P Van Dijck, et al. (eds.), *Theory and Practice of the European Convention on Human Rights* (Intersentia), 1-78. 2018.

Loucaides, Loukis G, 'Personality and Privacy under the European Convention on Human Rights', in Loukis G Loucaides (ed.), *Essays on the Developing Law of Human Rights* (Brill Nijhoff), 83-107. 1995.

McLnerney-Lankford, Siobhán, 'Legal methodologies and human rights research: Challenges and opportunities', in Bård-Anders Andreassen, H. O. Sano, and Siobhán McLnerney-Lankford (eds.), *Research methods in human rights: A handbook* (Cheltenham, United Kingdom: Edward Elgar Publishing), 38-67. 2017.

Milanovic, Marko, 'Extraterritoriality and human rights: prospects and challenges', in Thomas Gammeltoft-Hansen and Jens Vedsted-Hansen (eds.), *Human Rights and the Dark Side of Globalisation* (London: Routledge), 67-92. 2016.

Ovey, Clare, 'ECHR in Armed Conflict', in Katja S Ziegler, Elizabeth Wicks, and Loveday Hodson (eds.), *The UK and European Human Rights: A Strained Relationship?* (Bloomsbury Publishing). 2015.

Shelton, Dinah and Gould, Ariel, 'Positive and Negative Obligations', in Dinah Shelton (ed.), *The Oxford Handbook of International Human Rights Law* (Oxford University Press). 2013.

Smits, Jan, 'What is Legal Doctrine?: On the Aims and Methods of Legal-Dogmatic Research', in Rob van Gestel, Hans-W. Micklitz, and Edward L. Rubin (eds.), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (Cambridge University Press), 207-28. 2017.

Journal articles

Aswad, Evelyn Mary. 'The future of freedom of expression online', *Duke L. Tech. Rev.*, Vol. 17. 2018, p. 26.

Avila, Sandra. 'Implementing augmented reality in academic libraries', *Public Services Quarterly*, Vol. 13, No. 3. 2017, p. 190-99.

Besson, Samantha. 'The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to', *Leiden Journal of International Law*, Vol. 25, No. 4. 2012, p. 857-84.

Brown, Thackery I, et al. 'Prospective representation of navigational goals in the human hippocampus', *Science*, Vol. 352, No. 6291. 2016, p. 1323-26.

Cockfield, Arthur and Pridmore, Jason. 'A Synthetic Theory of Law and Technology', *Minnesota Journal of Law, Science and Technology (MJLST)*, Vol. 8, No. 2. 2007, p. 475-513.

Cockfield, Arthur J. 'Towards a law and technology theory', *Manitoba Law Journal*, Vol. 30, No. 3. 2003, p. 383.

Conoscenti, M., Vetrò, A., and Martin, J. C. De. 'Blockchain for the Internet of Things: A systematic literature review', *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. 2016, p. 1-6.

Constantiou, Ioanna D and Kallinikos, Jannis. 'New games, new rules: big data and the changing context of strategy', *Journal of Information Technology*, Vol. 30, No. 1. 2015, p. 44-57.

da Costa, Karen. 'Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy', *Human Rights Law Review*, Vol. 13, No. 2. 2013, p. 417-20.

Diggelmann, Oliver and Cleis, Maria Nicole. 'How the right to privacy became a human right', *Human Rights Law Review*, Vol. 14, No. 3. 2014, p. 441-58.

Dionisio, John David N, III, William G Burns, and Gilbert, Richard. '3D virtual worlds and the metaverse: Current status and future possibilities', *ACM Computing Surveys (CSUR)*, Vol. 45, No. 3. 2013, p. 1-38.

Dorsemaine, B., et al. 'Internet of Things: A Definition & Taxonomy', *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies.* 2015, p. 72-77.

Dotan, Maya, et al. 'Survey on blockchain networking: Context, state-of-the-art, challenges', *ACM Computing Surveys (CSUR)*, Vol. 54, No. 5. 2021, p. 1-34.

Fuster, Gloria González and Peeters, Michalina Nadolna. 'Person identification, human rights and ethical principles - Rethinking biometrics in the era of artificial intelligence', *Panel for the Future of Science and Technology.* 2021.

Gadekallu, Thippa Reddy, et al. 'Blockchain for the metaverse: A review', *arXiv preprint arXiv:2203.09738.* 2022.

Garon, Jon. 'Legal implications of a ubiquitous metaverse and a Web3 future', *Marq. L. Rev*, Vol. 106. 2022, p. 163.

Greenbaum, Dov. 'VR in the Prison System: Ethical and Legal Concerns', *AJOB Neuroscience*, Vol. 13, No. 3. 2022, p. 158-60.

Haijer, Friederycke and Ryngaert, Cedric. 'Reflections on Jaloud v. the Netherlands: jurisdictional consequences and resonance in Dutch society', *Journal of International Peacekeeping*, Vol. 19, No. 1- 2. 2015, p. 174-89.

Heller, Brittan. 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', *Vand. J. Ent. & Tech. L.*, Vol. 23. 2020, p. 1-51.

Huang, Y., Li, Y. J., and Cai, Z. 'Security and Privacy in Metaverse: A Comprehensive Survey', *Big Data Mining and Analytics*, Vol. 6, No. 2. 2023, p. 234-47.

Humble, Kristian P. 'International law, surveillance and the protection of privacy', *The International Journal of Human Rights*, Vol. 25, No. 1. 2021, p. 1-25.

Huo, Ru, et al. 'A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges', *IEEE Communications Surveys Tutorials*, Vol. 24, No. 1. 2022, p. 88-122.

Huxtable, Holly. 'E.T. Phoned Home...They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance', *Security and Human Rights*, Vol. 28, No. 1- 4. 2018, p. 92-112.

Huynh-The, Thien, et al. 'Artificial intelligence for the metaverse: A survey', *Engineering Applications of Artificial Intelligence*, Vol. 117. 2023.

Ivanova, Ekaterina and Borzunov, Georgii. 'Optimization of machine learning algorithm of emotion recognition in terms of human facial expressions', *Procedia Computer Science*, Vol. 169. 2020, p. 244-48.

Kalyvaki, Maria. 'Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction', *Journal of Metaverse*, Vol. 3, No. 1. 2023, p. 87-92.

Kanter, Theo. 'The metaverse and extended reality with distributed IoT', *IEEE Internet of Things Magazine*. 2021.

Lee, Lik-Hang, et al. 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda', *arXiv preprint arXiv:2110.05352*. 2021.

Li, Kai, et al. 'When Internet of Things Meets Metaverse: Convergence of Physical and Cyber Worlds', *IEEE Internet of Things Journal*. 2022.

Lubin, Asaf. 'Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)', *International Legal Materials*, Vol. 61, No. 4. 2022, p. 605-53.

Margulies, Peter. 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism', *Fordham L. Rev.*, Vol. 82. 2013, p. 2137.

Milanovic, Marko. 'Al-Skeini and Al-Jedda in Strasbourg', *European Journal of International Law*, Vol. 23, No. 1. 2012, p. 121-39.

Milanovic, Marko. 'Human rights treaties and foreign surveillance: Privacy in the digital age', *Harvard International Law Journal*, Vol. 56. 2015, p. 81-146.

Moncada, Jose A. 'Virtual reality as punishment', *Indiana Journal of Law and Social Equality*, Vol. 8. 2020, p. 304.

Nakamoto, Satoshi. 'Bitcoin: A peer-to-peer electronic cash system', *Decentralized Business Review*. 2008, p. 21260.

Park, S. M. and Kim, Y. G. 'A Metaverse: Taxonomy, Components, Applications, and Open Challenges', *IEEE Access*, Vol. 10. 2022, p. 4209-51.

Paust, Jordan J. 'Can You Hear Me Now: Private Communication, National Security, and the Human Rights Disconnect', *Chi. J. Int'l L.*, Vol. 15. 2014, p. 612.

Pietro, Roberto Di and Cresci, Stefano. 'Metaverse: Security and Privacy Issues', *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS- ISA)*. 2021, p. 281-88.

Reidenberg, Joel R. 'Technology and Internet Jurisdiction', *University of Pennsylvania Law Review*, Vol. 153, No. 6. 2005, p. 1951-74.

Ricanek, K. and Barbour, B. 'What Are Soft Biometrics and How Can They Be Used?', *Computer*, Vol. 44, No. 9. 2011, p. 106-08.

Ritter, Jeffrey and Mayer, Anna. 'Regulating data as property: a new construct for moving forward', *Duke L. Tech. Rev.*, Vol. 16. 2017, p. 220.

Ruggie, John Gerard. 'Business and human rights: the evolving international agenda', *American Journal of International Law*, Vol. 101, No. 4. 2007, p. 819-40.

Sandgren, Claes. 'Är rättsdogmatiken dogmatisk?', *Tidsskrift for Rettsvitenskap*, Vol. 118, No. 4/05. 2006, p. 648-56.

Sari, Aurel. 'Untangling Extra-Territorial Jurisdiction from International Responsibility in Jaloud v. Netherlands: Old Problem, New Solutions', *Military Law and Law of War Review*, Vol. 53, No. 2. 2014, p. 287-318.

Singh, Ms Neha. 'Criminal Jurisdiction in the Metaverse', *Journal of Survey in Fisheries Sciences*, Vol. 10, No. 1S. 2023, p. 4302-07.

Slobogin, Christopher and Brayne, Sarah. 'Surveillance Technologies and Constitutional Law', *Annual Review of Criminology*, Vol. 6, No. 1. 2023, p. 219-40.

Solove, Daniel J. 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*, Vol. 154, No. 3. 2006, p. 477-564.

Stokel-Walker, Chris. 'Welcome to the Metaverse', *New Scientist*, Vol. 253, No. 3368. 2022, p. 39- 43.

Van Den Broek, Egon L, et al. 'Affective man-machine interface: Unveiling human emotions through biosignals', *Biomedical Engineering Systems and Technologies: International Joint Conference (BIOSTEC 2009)*. 2010, p. 21-47.

Wachter, Sandra and Mittelstadt, Brent. 'A right to reasonable inferences: re-thinking data protection law in the age of big data and AI', *Colum. Bus. L. Rev.* 2019, p. 494.

Wang, Y., et al. 'A Survey on Metaverse: Fundamentals, Security, and Privacy', *IEEE Communications Surveys & Tutorials*. 2022.

Watt, Eliza. 'The role of international human rights law in the protection of online privacy in the age of surveillance', *2017 9th International Conference on Cyber Conflict (CyCon)*. 2017, p. 1-14.

Whitman, James Q. 'The Two Western Cultures of Privacy: Dignity versus Liberty', *The Yale Law Journal*, Vol. 113, No. 6. 2004, p. 1151-221.

Zuboff, Shoshana. 'Big Other: surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology*, Vol. 30, No. 1. 2015, p. 75-89.

Theses

Wide, Erica, 'Exporting Privacy - A Study on the Extraterritorial Application of the European Convention on Human Rights to Foreign Mass Surveillance' (Master Thesis, Lund University, 2020).

Government, legal & company documents

United Nations General Assembly, *The right to privacy in the digital age - Resolution adopted by the Human Rights Council on 26 September 2019*, 2019. (A/HRC/RES/42/15).

The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Facial Recognition*, 2021. (T-PD(2020)03rev4).
https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (Accessed 2023-03-14).

European Court of Human Rights, *Guide to the Case-Law of the of the European Court of Human Rights - Data protection*, 2022.
https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf (Accessed 2023-05-15).

European Court of Human Rights, *Guide on Article 1 of the European Convention on Human Rights: Obligation to respect human rights – Concepts of "jurisdiction" and imputability*, 2022. https://www.echr.coe.int/documents/guide_art_1_eng.pdf (Accessed 2023-02-28).

Meta, *Terms of Service*, 2023. https://www.facebook.com/legal/terms (Accessed 2023-04-26).

Press releases

Meta, 'Facebook to Establish International Headquarters in Dublin, Ireland'. Press release 2008- 10-02.
https://about.fb.com/news/2008/10/facebook-to-establish-international-headquarters- in-dublin-ireland/

Rimol, Meghan, 'Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026'. Press release 2022-02-07. Gartner.
https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25- percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026

Newspaper articles

Davies, Caroline, 'Welcome to your virtual cell: could you survive solitary confinement?', The Guardian, 2016.

Gash, Tom, 'Forget prisons, the future of punishment will be virtual', Wired, 2020.

Gellman, Barton and Poitras, Laura (2013), 'NSA slides explain the PRISM data-collection program', The Washington Post.

Isaac, Mike (2021), 'Facebook Renames Itself Meta', The New York Times.

Rosenberg, Matthew, Confessore, Nicholas, and Cadwalladr, Carole (2018), 'How Trump Consultants Exploited the Facebook Data of Millions', The New York Times.

Web pages

'Biometrics', *The Electronic Frontier Foundation (EFF)*.
https://www.eff.org/issues/biometrics. (Accessed 2023-03-15).

'Mass surveillance - Which countries could have access to your data?', *Amnesty International UK*. 2015.
https://www.amnesty.org.uk/which-countries-access-your-data-nsa-gchq-five-eyes- snowden-surveillance. (Accessed 2023-03-05).

Copeland, Christopher and Michl, Kyle, 'Research Report: Government enters the metaverse', *Accenture Federal Services - Federal Technology Vision 2022*. 2022-09-12.
https://www .accenture.com/us-en/insightsnew/us-federal-government/technology-vision-2022. (Accessed 2023-01-25).

Drapkin, Aaron, 'Metaverse Companies: Who's Involved and Who's Investing in 2022', *tech.co*. 2023-01-24.
https://tech.co/news/metaverse-companies-whos-involved-whos-investing. (Accessed 2023-02-05).

Elmasry, Tarek, et al., 'Value creation in the metaverse - The real business of the virtual world', *McKinsey & Company*. 2022-06-14.
https://www.mckinsey.com/capabilities/growth-marketing- and-sales/our-insights/value-creation-in-the-metaverse. (Accessed 2023-01-01).

Feltham, Jamie, 'HoloLens 2 Review: Ahead Of Its Time, For Better And Worse', *Upload*. 2021- 04-09. https://www.uploadvr.com/hololens-2-review/. (Accessed 2023-05-12).

Johnson, Shawn, 'Centralized and Decentralized Metaverse: What's the Difference?', *BusinessNews*. 2023-01-22. https://biz.crast.net/centralized-and-decentralized-metaverse-whats-the-difference-cryptosaurus/. (Accessed 2023-05-12).

Opsahl, Kurt, 'Come Back with a Warrant for my Virtual House', *The Electronic Frontier Foundation (EFF)*. 2020-10-05.
https://www.eff.org/deeplinks/2020/10/come-back-warrant-my-virtual- house. (Accessed 2023-03-14).

Radoff, Jon, 'The Metaverse Value-Chain', *Medium.com*. 2021-04-07.
https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7. (Accessed 2023-02-07).

Rodriguez, Katitza and Mir, Rory, 'If Privacy Dies in VR, It Dies in Real Life', *The Electronic Frontier Foundation (EFF)*. 2020-08-25.
https://www.eff.org/deeplinks/2020/08/if-privacy-dies- vr-it-dies-real-life. (Accessed 2023-03-15).

Rodriguez, Katitza and Opsahl, Kurt, 'Augmented Reality Must Have Augmented Privacy', *The Electronic Frontier Foundation (EFF)*. 2020-10-16.
https://www .eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy. (Accessed 2023-03-14).

Rodriguez, Katitza and Mir, Rory, 'Pivotal Year for the Metaverse and Extended Reality: 2022 in Review', *The Electronic Frontier Foundation (EFF)*. 2022-12-24.
https://www .eff.org/deeplinks/2022/12/pivotal-year-metaverse-and-extended-reality . (Accessed 2023-05-12).

Strickland, Jonathan, 'How Virtual Reality Gear Works', *HowStuffWorks*.
https://electronics.howstuffworks.com/gadgets/other-gadgets/VR-gear.htmpt6. (Accessed 2023-03-10).

Movies & broadcasts

The Social Dilemma (Netflix, 2020), Orlowski, Jeff (dir.).