the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

EUROPE

Regional Coordinators:
Albert Agustinoy *Cuatrecasas, Barcelona*
Eric Wagner *Gleiss Lutz, Stuttgart*

Introduction

Magda Cocco *Vieira de Almeida, Lisbon*
Iakovina Kindylidi *Vieira de Almeida, Lisbon*

Purpose of the guideline policy – scope, updates (annually)

The purpose of this metaverse guide is to provide the readership, primarily consisting of in-house counsels and regulators, with an overview of the legal framework applicable to the metaverse and proper guidance in this regard, recognising the evolving nature of regulations that may impact the metaverse across various jurisdictions. Indeed, we acknowledge that a 'deep dive' into the regulation in different jurisdictions will not be possible due to the dynamic, international regulatory landscape surrounding the metaverse. We will therefore limit ourselves to an overview of national and European law that does not claim to be exhaustive.

What is the metaverse: convergence of technologies, key characteristics and state of the metaverse market?

There is no fixed definition for the metaverse, which is why it has to be paraphrased. The term 'metaverse' is made up of the word parts 'meta' and 'universe'. While 'universe' refers to an independent, expansive space, 'meta' lends this space a transcending reference, so that the metaverse can be described as a virtual, simulated and interactive 3D ecosystem that interacts with the real, physical world and enables a variety of virtual activities to be carried out realistically through avatars that embody the user. The metaverse ecosystem is interoperable as part of Web 3.0: ie, it consists of several interwoven and interconnected platforms designed by different providers and programs, and allows users to immerse themselves in an independent, digital environment in such a way that 'awareness of the "real" world recedes into the back-ground', creating immersive experiences. To enjoy the latter, virtual reality (VR), augmented reality (AR) or mixed reality (MR) technologies are required, while the metaverse itself is based on a complex technical construction based on blockchains, smart contracts and distributed ledger technologies (DLT), among others. The promising metaverse is at the beginning of its development and offers endless possibilities, functions and opportunities in terms of social and, above all, economic aspects that are still far from being fully developed, which opens up new dimensions for companies in particular — in the truest sense of the word. While experts expect the metaverse to be worth almost US$800bn by 2025, it could be worth up to US$5tn by 2030.

Due to its decentralised organisation and interoperability, the metaverse ecosystem is made up of several independent platform operators who interweave their platforms so that they form the metaverse as a whole. The platform operators thus represent the ground, basis, foundation and prerequisite for the realisation of the metaverse. The metaverse then becomes the sphere of action for its users, who are represented by their avatars – ie, digital puppets – and can carry out a variety of different activities realistically. This includes, for example, attending concerts or lectures, shopping centres or even, as in our case, law firms, making the metaverse a place for social and business encounters. Third-party developers and companies exploit the latter by developing their own buildings, events or business premises with the help of technical interfaces and implementing them through the use of such platforms. The users, embodied by their avatars, can take advantage of the economically versatile and innovative offers, pay a certain amount of money for this — (also) in the real world — and thus become not only guests or customers, but also consumers worthy of protection. Above all, the economic synergies and dynamics are still at the beginning of their development and will present the existing legal system with many as yet unknown challenges.

Data

Magda Cocco *Vieira de Almeida, Lisbon*
Iakovina Kindylidi *Vieira de Almeida, Lisbon*

Q 1. Are there any data (personal and non-personal) policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Although not explicitly referring to the metaverse, several EU policies, strategies and regulations apply to personal and non-personal data in virtual environments. While an exhaustive list exceeds the scope of this chapter, the most important applicable strategies and regulations are as follows.

Personal data

The General Data Protection Regulation (GDPR)[1] establishes principles and rules for safeguarding individuals' rights regarding their personal data. It applies to the processing of personal data by controllers and processors established in the European Union, regardless of whether the processing takes place within the EU or not. It also applies to the processing of personal data of individuals who are in the EU, irrespective of the location of the controller or processor. In other words, the GDPR applies extraterritorially to organisations located outside the EU if they offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU.

The ePrivacy Directive[2] regulates the security of electronic communications data and the use of tracking technologies. The ePrivacy Directive applies to providers of electronic communication services, including internet service providers, telecommunications companies, email service providers and messaging app developers. It also applies to entities involved in the processing of electronic communications data, such as website operators that use cookies or similar tracking technologies. It applies to entities established in the EU that provide electronic communication services, regardless of whether the processing of personal data occurs within the EU or not. Additionally, it applies to the processing of electronic communications data of individuals located in the EU, regardless of the location of the entity processing the data. Like the GDPR, the ePrivacy Directive may also have extraterritorial application in certain circumstances.

Both personal and non-personal data

The Data Governance Act[3] aims to increase the amount of data available and strengthen data sharing from public to private entities, while it also aims to establish a framework for trustworthy data intermediaries and data altruism organisations. It applies to EU public sector bodies, data intermediaries and data altruism organisations.

The Data Act complements the Data Governance Act by clarifying the entities permitted to derive value from data and the conditions under which they may do so, while also establishing a framework for data sharing within the European Common Data Spaces. It delineates harmonised regulations regarding data generated by the utilisation of related products or services, such as Internet of Things (IoT) devices, stipulating the rights of data holders to share such data with recipients and public sector bodies or EU institutions, agencies or bodies in instances of exceptional necessity for the performance of tasks conducted in the public interest.

The Act imposes obligations on various stakeholders including manufacturers of products and providers of associated services distributed within the EU market, users of said products or services, data owners facilitating data access to recipients within the EU, recipients within the EU receiving such data, public sector bodies and EU institutions, agencies or bodies soliciting data holders to provide data under exceptional circumstances for tasks conducted in the public interest,

1 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 [2016] OJ L119/1
2 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.
3 Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L152/1.

and data holders complying with such requests. Additionally, it pertains to providers of data processing services catering to customers within the EU.

The Common European Data Spaces in strategic sectors and domains of public interest for the European Single Market aims to promote accessibility and data quality.

Non-personal data

Regulation on a framework for the free flow of non-personal data in the EU facilitates the free flow of non-personal data across borders within the EU's internal market and applies to providers of data processing services offering data processing services in the EU, irrespective of whether the provider is established and to EU-based users of data processing services.

Together, these frameworks provide a comprehensive data protection framework for the processing and movement of personal data within the metaverse, ensuring individuals' privacy rights are upheld in emerging virtual landscapes.

Q 2. How are the various personal and non-personal data associated with the metaverse protected in your jurisdiction?

Metaverse technologies leads to the generation of new types of both personal and non-personal data, raising new regulatory challenges. From body-based to inferred data and electroencephalograms (EEGs) for brain–computer interfaces, the new sensitive types of data may blur traditional boundaries and necessitate re-evaluation of the current privacy norms.

Although not specifically referring to data in the metaverse or to novel data categories, the current applicable data (personal and non-personal) rules offer a comprehensive framework for the protection of data in the metaverse, including data of users, devices and third parties, and avatars, synthetic and inferred data.

Notwithstanding the above, avatars, synthetic data and inferred data generated within the metaverse may raise unique privacy concerns that the current framework is not in a position to address or they are exacerbating existing challenges due to their convergence with other emerging technologies, such as AI (see the chapter on AI in the metaverse for a more detailed overview of the AI-related challenges in the metaverse) and blockchain. In any case, to the extent that these forms of data are linked to identifiable individuals or contain sensitive information, they would be subject to the GDPR's protections for personal data.

Moreover, it should be noted that there is no guidance specific for metaverse-related data that has been issued by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS). However, it should be noted that the following reports are particularly relevant, amongst others as they may indicate the possible future approach that will be followed in Europe regarding the shape of personal data protection in the metaverse in the future:

- EDPS, Technology report No 1 – Smart glasses and data protection, January 2019;
- EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement;
- EDPB, Guidelines 3/2022 on dark patterns in social media platform interfaces: how to recognise and avoid them;
- EDPB, Guidelines 02/2021 on virtual voice assistants;
- EDPB, Guidelines 08/2020 on the targeting of social media users; and
- EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

Lastly, there is no case law regarding metaverse-related data by the EU.

Q 3. Who are the different stakeholders involved in the data value chains in the metaverse and in the case of personal data their data protection roles? How are their activities regulated under regional/ national policies, strategies or regulations?

Considering the manifold technologies and activities involved in the metaverse, the metaverse data value chain is particularly complex, extending to various metaverse stakeholders that engage with and support activities in the metaverse.

The different stakeholders involved in the data value chains in the metaverse may include users, content creators, platform providers, service providers, data intermediaries, data brokers, data analysts, regulators and researchers. Depending on the nature and purpose of the data processing and the type of data involved, they may have different data protection roles, such as:

- data subjects, data controllers, data processors and sub-processors or joint controllers, as defined by the GDPR;
- data intermediaries, data altruism organisers as defined in the Data Governance Act; or
- manufacturers, users and service providers covered by the Data Act.

Accordingly, depending on the nature of the stakeholder's activities, they may be subject to different rules and obligations. Considering that the same stakeholder may assume multiple data-related roles, a case-by-case analysis and a clear mapping of data flows is necessary.

Q 4. In relation to personal data, what are the data protection principles (eg transparency) applicable in the metaverse? What are the most common types of infringement of data protection principles in the metaverse (eg data minimisation) in your jurisdiction?

Notwithstanding any infringements that were made public from specific Member States, and considering the risks associated with the technology, the most common types of infringement of data protection principles in the metaverse may include:

- lack of valid consent or legal basis for data processing;
- excessive or unnecessary collection or retention of data;
- insufficient or misleading information or communication to data subjects;
- inadequate security measures or data breach incidents;
- unlawful or unauthorised data sharing or transfer; and
- failure to respect data subjects' rights, such as the right to access, rectify, erase or port data.

Moreover, from a perspective of non-personal data, there is no specific information on data-related infringements. However, considering the particularities of the metaverse, some of the most common types of infringement may include:

- unauthorised extraction or re-utilisation of the contents of a protected database;
- misappropriation or disclosure of trade secrets or confidential information;
- infringement or circumvention of intellectual property rights or contractual terms; and
- unfair competition or parasitic practices.

The personal data protection principles applicable in the metaverse are the same as those established by the GDPR, namely lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

The sanctions that may apply to these infringements could range from civil remedies, such as injunctions, damages or restitution, to criminal penalties, such as fines, imprisonment or confiscation or administrative sanctions, such as warnings, orders, fines or bans, depending on the severity and impact of the offence, and the applicable national law. In the case of GDPR, fines reaching up to €20m or up to four per cent of the total worldwide turnover of the preceding financial year, whichever is higher, may apply.

There is no case law or decision of a regulator regarding ownership of digital assets in the metaverse in the EU region, as this is a novel and emerging area.

Q 5. In relation to non-personal data, how is data sharing/licensing regulated in your jurisdiction? Is data ownership recognised? How is proprietary information, including any rights to datasets regulated in your jurisdiction? What are the most common types of infringement of these rules in the metaverse (eg unlawful use of proprietary information) in your jurisdiction?

Data sharing/licensing of data is not regulated as such: it is usually regulated contractually. Nonetheless, some data-sharing activities, depending on the data-related role of the stakeholder and the nature of the data, may be subject to the rules set out in the Data Governance Act and the Data Act. Both regulations have introduced mechanisms to facilitate the sharing of certain categories of data (personal and non-personal).

Data ownership is not explicitly recognised by EU law, as information is not protected by a property right. However, data may be subject to other types of rights or interests, such as intellectual property rights, contractual rights, database rights or trade secrets. In addition to these possible rights, rights of the data subjects on their rights should also be considered.

The most common types of infringement of these rules in the metaverse may vary depending on the specific sector, service or application involved, but some examples could include:

- unfair or misleading commercial practices, unfair terms and conditions or lack of information or consent;
- infringement of personal data protection rights, such as unlawful collection, processing or sharing of personal data or lack of security or transparency measures; and
- infringement of intellectual property rights.

The sanctions that may apply to these infringements could range from civil remedies, such as injunctions, damages or restitution, to criminal penalties, such as fines, imprisonment or confiscation or administrative sanctions, such as warnings, orders, fines or bans, depending on the severity and impact of the offence, and the applicable national law. In the case of GDPR, fines reaching up to €20m or up to 4 per cent of the total worldwide turnover of the preceding financial year, whichever is higher, may apply.

There is no case law by the European Court of Justice (ECJ) regarding infringements of these rules in the metaverse, as this is a new and evolving phenomenon. In any case, there may be relevant decision by the ECJ that may be used as a basis to determine the approach that will be followed for regulating infringement of these rules.

Q 6. Are there any policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?

There are several policies/strategies/regulations applicable to digital marketing in the metaverse in the EU, such as the ePrivacy Directive, the Unfair Commercial Practices Directive[4] and the Consumer Rights Directive,[5] among others.

These regulations are complemented by national laws, especially advertising laws and codes, self-regulatory advertising practices and sector-specific rules, depending on the product/service being advertised or on the means of dissemination, such as the Audiovisual Media Services Directive[6] and the Digital Services Act.

The sanctions that may apply for digital marketing infringements in the metaverse are the same as those provided by the relevant EU laws, which include civil remedies, such as injunctions, damages or termination of contracts; criminal penalties, such as fines or imprisonment, in cases of fraudulent or misleading practices; and administrative sanctions, such as fines, warnings or orders to cease or correct the infringement; subject to the applicable national laws. In addition, when the digital marketing practice also infringes the GDPR, administrative fines may reach up to €20m or up to four per cent of the total worldwide turnover of the company for the previous financial year, whichever is higher.

There is no case law by the ECJ regarding infringements of these rules in the metaverse, as this is a new and evolving phenomenon. In any case, there may be relevant decisions by the ECJ regarding digital marketing that may be used as a basis to determine the approach that will be followed for regulating infringement of these rules.

Q 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring the protection of minors' data? What is the age of consent for data protection purposes? Is it necessary to verify the consent provided by a responsible adult?

There are some policies, strategies and regulations in the EU which are focused on ensuring the protection of minors' data, such as the GDPR, the ePrivacy Directive and the Better Internet for Kids Strategy.

Under Article 8 of the GDPR, the processing of personal data for the purposes of an information society service directly offered to a minor under 16 years old is lawful only if consent is given or authorised by the holder of parental responsibility. However, the GDPR also allows Member States to lower this age limit, but not below 13 years old. Therefore, the age of consent may vary from 13 to 16 years old depending on the national law of each Member State. The GDPR requires data controllers to make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility, taking into consideration the available technology.

Q 8. How are international data transfers regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of these rules in your jurisdiction?

A study conducted in 2021 by the Information Technology and Innovation Foundation (ITIF) revealed that 62 countries impose bans or restrictions on cross-border data flows, and the rate at which these restrictions are being implemented is accelerating.

4 Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC and Regulation (EC) 2006/2004 [2005] OJ L149/22.

5 Directive 2011/83/EU on consumer rights, amending Directive 93/13/EEC and Directive 1999/44/EC and repealing Council Directive 85/577/EEC and Directive 97/7/EC [2011] OJ L304/64.

6 Directive (EU) 2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2018] OJ L303/69.

International data transfers are regulated by the GDPR, which requires that personal data transferred to third countries or international organisations must ensure an adequate level of protection or be subject to appropriate safeguards, such as standard contractual clauses, binding corporate rules or codes of conduct, and other adequate supplementary measures.

The GDPR also provides derogations for specific situations, such as consent, contractual necessity or public interest. The European Commission is responsible for adopting adequacy decisions for third countries or international organisations that provide a level of protection equivalent to the EU.

Without prejudice to additional relevant guidelines, the EDPB has issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. These guidelines are also complemented by guidance provided by various national data protection authorities (DPAs).

There is some case law that has been issued by the ECJ regarding infringements of these rules in the EU region, although not specifically related to the metaverse. For example, the ECJ has ruled on several cases involving the interpretation and application of the GDPR and the ePrivacy Directive in relation to international data transfers, such as, most notably, the *Schrems I and Schrems II* cases[7] on the invalidation of the EU–US Safe Harbour and Privacy Shield frameworks, and the *Privacy International* case regarding access to electronic communications data by national security agencies. These decisions are further complemented by decisions issued by national DPAs regarding international data transfers.

Q 9. How is automated decision-making regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of the rules applicable to automated decision-making in your jurisdiction?

AI is one of the pillars for the realisation of the metaverse. See the chapter on AI and the metaverse for further details on the EU approach to AI in the metaverse.

Automated decision-making is regulated under Article 22 of the GDPR. The GDPR sets out the rights and obligations related to the processing of personal data that involves solely automated decision-making, including profiling, which produces legal effects or similarly significant effects on the data subject. The GDPR provides that such processing is generally prohibited unless it is authorised by an EU or Member State law; necessary for the performance of a contract; or based on the explicit consent of the data subject. In any case, the GDPR requires data controllers to implement suitable safeguards to protect the data subject's rights and freedoms and legitimate interests, such as the right to obtain human intervention, to express their point of view, to contest a decision and to be informed of the logic involved.

The Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018 by the EDPB, provides further guidance as to the interpretation of Article 22.

In addition, further data-related obligations are introduced by the AI Act[8] and these will also impact AI-based decisions.

There is some case law by the ECJ regarding infringements of these rules in the EU region, although not specifically related to the metaverse – for example, *SCHUFA Holding*.[9] These decisions are further complemented by decisions issued by national DPAs regarding international data transfers.

Q 10. What rights are granted to individuals for protecting their rights in the metaverse and how can they exercise them? What is the level of enforcement based on private claims in your jurisdiction?

7 *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:650, [2016] Q.B. 527 (*'Schrems I'*) and *Data Protection Commissioner v Facebook Ireland Ltd* (C-311/18) EU:C:2020:559, [2021] 1 W.L.R. 751 ('Schrems II').

8 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

9 (C-634/21) (ECHR, 7 December 2023).

Although not explicitly referring to the metaverse, the GDPR sets out the following rights for data subjects:

- *Right to access:* individuals have the right to obtain confirmation as to whether personal data concerning them is being processed, and if so, be provided with access to that data and certain information about how it is processed.
- *Right to rectification:* individuals have the right to request the correction of inaccurate personal data concerning them.
- *Right to erasure (right to be forgotten)*: individuals have the right to request the deletion of their personal data under certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or processed.
- *Right to restriction of processing*: individuals have the right to restrict the processing of their personal data under certain circumstances, such as when they contest the accuracy of the data or the lawfulness of the processing.
- *Right to data portability*: individuals have the right to receive their personal data in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller.
- *Right to object*: individuals have the right to object to the processing of their personal data in certain situations, such as for direct marketing purposes.
- *Rights in relation to automated decision-making and profiling*: individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

To exercise these rights in the context of the metaverse, individuals would likely need to engage with the platforms or service providers operating within the metaverse environment. This may involve submitting requests through the platform's interface or contacting the respective organisation.

Regarding enforcement based on private claims in Europe, individuals have the right to lodge complaints with the relevant DPA if they believe their rights under the GDPR have been violated. DPAs have the power to investigate complaints, issue warnings, impose administrative fines and order corrective measures in regard to organisations found to be in violation of the GDPR.

The level of enforcement based on private claims may vary depending on factors such as the severity of the violation, the cooperation of the organisation involved, the specific circumstances of the case and the approaches followed by the national DPA.

In relation to non-personal data, without prejudice to specific rules, especially in relation to trade secrets, rights are usually regulated contractually.

Q 11. Are there any upcoming policies, strategies or regulations that will impact the use of data in the metaverse?

Over the past three years, both the European Commission and European Parliament have been actively releasing reports and studies regarding the metaverse and digital assets within the context of Web 4.0 and virtual environments. While providing an exhaustive list of these reports and initiatives is beyond the scope of this discussion, one of the latest policies published by the European Commission is entitled *An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the Next Technological Transition,* issued in July 2023.[10] Additionally, in January 2024, the European Commission initiated a public consultation on competition within virtual worlds.

These two initiatives illustrate the Commission's interest in potentially regulating virtual worlds in the medium term, which could significantly influence how data use is regulated across the EU.

10 *An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the Next Technological Transition* (European Commission, July 2023).

Aside from anticipating the outcomes of the public consultation on competition in virtual worlds and potential initiatives stemming from the European Commission's communications, the implementation of the three pillars of the EU's Data Strategy – the European Data Governance Act, the Data Act and Common Data Spaces initiatives – could potentially impact digital transactions in the metaverse in terms of how data is shared, accessed and used by different actors, such as data intermediaries, data altruism organisations or public sector bodies.

Considering the convergence of metaverse and AI technologies, the recently approved Artificial Intelligence Act (AIA) is of particular importance. The AIA could potentially affect digital transactions in the metaverse in terms of how AI systems are classified, assessed and monitored for compliance with ethical and legal standards, as well as how users are informed and protected from potential harms or biases. See the chapter on AI and the metaverse for further information on the EU approach to AI in the metaverse.

Cybersecurity

Albert Agustinoy *Cuatrecasas, Barcelona*

Q 1. Are there any cybersecurity policies, strategies or regulations applicable to the metaverse in your jurisdiction?

There are no specific cybersecurity policies, strategies or regulations applicable to the metaverse in the EU region. However, the EU authorities have already adopted several policy papers which address cybersecurity issues connected with the metaverse.

Namely, in the European Parliament briefing dated June 2022 named *Metaverse: Opportunities, risks and policy implications* (the 'EU Parliament Metaverse Briefing'),[11] reference is made to cybersecurity being one of the top issues to be addressed in the future regulation of immersive environments. In this respect, the European Parliament considers that constructing a safe environment for the metaverse will be one of the key regulatory goals in the EU, due to threats which are already present, such as phishing, malware and hacking. In this respect, reference is made to the need to protect the integrity of avatars and hamper new forms of cybercrime, such as the sale of fake non-fungible tokens (NFTs), illegal use of cryptocurrencies and malicious smart contracts.

Similarly, in the Communication from the European Commission dated 11 July 2023, *An EU initiative on WEB 4.0 and virtual worlds: a head start in the next technological transition* (the 'Commission's Communication on Virtual Worlds'),[12] cybersecurity is mentioned as one of the elements to be included in a future so-called 'toolbox' for the management by citizens of their virtual identities, assets and data in immersive environments. In a similar way, the said Communication also makes reference to the need to define, in the upcoming years, a major investment policy for the development, among other elements, of cybersecurity technologies for virtual worlds.

Apart from these policy papers, which should shape the future regulatory developments in this field in regard to cybersecurity in the metaverse, some existing or proposed EU regulations have implications for cybersecurity in the metaverse. In particular, reference should be made to the following regulations:

- the GDPR, which defines a number of cybersecurity-related obligations that certainly apply to the metaverse. These duties would include the following at the very least: (1) a general and overall obligation to ensure the protection of data related to individuals; (2) a duty to notify to the relevant authorities – and the affected users, in case of high risk for them – of any security breach impacting personal data; and (3) an obligation to ensure, at all times, the exercise by the individuals whose data is processed of the rights granted in the regulation in their favour.

- the Digital Services Act and the Digital Markets Act, which among the duties applicable to the platform operators category where metaverse platforms would be included, specific cybersecurity obligations would be invocable. In that respect, the regulations contemplate obligations such as: (1) the implementation of security measures aimed at protecting the personal information and security of users; (2) the identification and erasure of illegal content; (3) any transparency duties in regard to online advertising; (4) the protection of personal data in general; and (5) a duty to provide to technical compatibility with other technologies and access to relevant data third parties.

- the Data Governance Act and the Data Act, which also contemplate cybersecurity duties connected with immersive digital environments, such as the following: (1) data security, ensuring protection against non-authorised access to information as well as against the destruction and/or loss of data; (2) transparency and liability, requiring companies involved in the processing of great amounts of data (such as metaverse platform operators) to be transparent vis-à-vis their processing procedures and be liable in case of any security breach; and (5) access and control of data, guaranteeing that the users who generate data are entitled to access and have control of the information they generate in such environments.

11 European Parliament Briefing, 'Metaverse: Opportunities, risks and policy implications' (European Parliament, June 2022).
12 European Commission, An EU Initiative on WEB 4.0 and virtual worlds: a head start in the next technological transition (11 July 2023).

The AI Act defines a number of cybersecurity duties that will apply to AI-based tools being used in the metaverse. In particular, the following obligations should be highlighted:

- *general security*, on the basis of which designing and operating any such tool should be made pursuant to secure and operative conditions and in compliance with the security standards defined by EU regulations;
- *risk assessment*, requiring any AI developer to execute a risk assessment exercise before the deployment of the corresponding tool;
- *transparency and explainability*, ensuring that AI systems are transparent in their functioning and provide clear explanations on decisions and actions having been taken by the system being used; and
- *oversight and control*, requiring that any AI system can be monitored and audited and making eventual human intervention possible in order to address any situation that may derive from the use of AI systems.

Q 2. What are the security-by-design (physical and digital interfaces) principles applicable to the metaverse in your jurisdiction?

Fundamental rights, safety and security are guiding principles for the development of virtual worlds, which includes security-by-design approaches. Apart from the obligations mentioned under question 1, the security-by-design principles contained in the Cyber Resilience Act,[13] which — among other products — applies to software development. This regulation provides for the liability of manufacturers for a product's cybersecurity throughout its whole lifecycle; the transparency and information provided to consumers about the cybersecurity of the products; and the standardisation for the interoperability between different platforms and networks, which includes cybersecurity standards. Moreover, the Cyber Resilience Act includes data protection requirements for these products in line with the guiding principles of the GDPR, such as data minimisation, and the confidentiality and integrity of the data being saved, transmitted or otherwise processed.

Apart from the above, the European Parliament has defined, in its EU Parliament Metaverse Briefing, a number of general principles for designing secure metaverse environments. Namely, the following have been proposed for consideration in the future regulations dealing with this matter:

- the security of metaverse-enabling devices;
- security of protocols to mitigate the risk of transfer of harmful content between platforms and enabling free movement of users between virtual platforms; and
- avatar integrity, aimed at avoiding risks deriving from duplication and interoperability misuse.

Q 3. Have there been any cyber incidents in the metaverse in your jurisdiction? How do any related policies, strategies or regulations react to cyber incidents?

Until now, no specific major cyber incidents in the metaverse in the EU region have taken place. However, as previously indicated, cybersecurity challenges and risks in the metaverse may include phishing, malware, hacking, identity theft, avatar misuse, cybercrime and data breaches.

EU regulations may lead to liabilities for online platforms, data processors, AI providers and digital product and service providers. Under these regulations, the sanctions that may apply to cyber incidents in the metaverse could depend on the nature and severity of the incident, the applicable regulation and the jurisdiction involved, and they could include fines, penalties, injunctions, damages or criminal charges. For instance, sanctions under the Cyber Resilience Act for non-compliance with the essential cybersecurity requirements can include monetary fines of up to €15m or 2.5 per cent of a company's total annual worldwide turnover.

13 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

Outside the scope of the metaverse, some of the most recent cases regarding cyber incidents in the EU region include: the €6.5m fine imposed by the Spanish Data Protection Authority in case EXP202305587 in regard to Iberdrola, due to a cyberattack that leaked the sensitive data of over 1.3 million clients in 2022, and the €3.1m fine imposed on Abanca by the European Central Bank (ECB) for the undue delay in regard to the notification of a cyberattack in 2019.

Q 4. Are there any cybersecurity standards in your jurisdiction specifically applicable to the metaverse? What are the main obligations they set out?

The European Cybersecurity Certification Scheme is the first scheme to be adopted under the Cybersecurity Act certification framework and it is based on the international standard known as the Common Criteria for Information Technology Security Evaluation.[14] The Implementing Act for this certification scheme was published by the European Commission on 31 January 2024. The scheme applies on a voluntary basis in the EU and focuses on certifying the cybersecurity of ICT products (software and hardware) throughout their lifecycle, and it is expected to complement the Cyber Resilience Act.

Within the framework of the Common Criteria, the process of certification involves evaluating the product against a security target (which includes a description of the security issues related to the ICT product, along with the security goals that aim to mitigate these issues). To address these security issues and meet the security goals, a given collection of Security Requirements is established for the ICT product, thus following a risk-based criteria.

Q 5. Are there any upcoming policies, strategies or regulations that will impact cybersecurity in the metaverse?

Regarding future regulation that may impact cybersecurity in the metaverse, the European Parliament acknowledged that the applicable legal frameworks in regard to the following areas may affect the regulation of the metaverse, such as blockchain and smart contracts (MiCA Regulation[15]), product safety (General Product Safety Regulation[16]), cybersecurity resilience (Cyber Resilience Act), digital operational resilience (Digital Operational Resilience Act (DORA)[17]), and markets in crypto assets (MiCA Regulation). Moreover, as previously indicated, EU institutions have already published policy papers, which will likely lead to legislative proposals in the short and medium term.

Apart from the above, according to the EU Parliament's Metaverse Briefing, the definition and implementation of future regulations in regard to the metaverse in the EU should ensure the following regulatory goals are met:

- define a legal framework for blockchain and smart contracts in order to guarantee the protection of users' identities in the metaverse and prevent fraud;
- consolidate an EU cyber resilience capacity, supplementing the measures already contemplated in the MiCA Regulation, DORA, the Cyber Resilience Act and the NIS2 Directive.[18]
- improve the education of users in this field by updating the digital education action plans.

14 Common Criteria (ISO/IEC 15408 and ISO/IEC 18045).
15 Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L150/40.
16 Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) 1025/2012 and Directive (EU) 2020/1828 and repealing Directive 2001/95/EC and Directive 87/357 [2023] OJ L135/1.
17 Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 [2022] OJ L333/1.
18 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 [2022] OJ L333/80.

Digital identity and authentication

Albert Agustinoy *Cuatrecasas, Barcelona*

Q 1. What are the different types of digital identity in the metaverse: what are the different tiers and types of ID and what are the different levels of protection in your jurisdiction?

There are several digital identity and authentication policies, strategies and regulations already in place that are applicable to the metaverse in the EU. Some of the most relevant ones are the eIDAS Regulation,[19] which establishes a framework for electronic identification and trust services in the EU, and its proposed amendment, which aims at introducing a European digital identity framework and digital wallet for cross-border and cross-sector use.

Additionally, other EU regulations already define duties in this respect:

- the GDPR contemplates the following obligations on this matter: (1) lawful processing, requiring from the operator the processing of data from the user ensuring all the guarantees, rights and legal basis defined in the GDPR itself; (2) guaranteeing the rights of users in regards to their data – namely, access, rectification, erasure, restricting processing, data portability and the right not to be subject to a decision based solely on automated processing; and (3) protection of sensitive data;
- the Digital Services Act, which sets out the rules on the following obligations for platform operators: (1) verification of identity when users access and use the corresponding digital services; and (2) providing users with access to their digital identity, on the basis of which users shall be granted the right to count with their own digital identity and manage it pursuant to their preferences; and
- the Data Governance Act and the Data Act define the following relevant obligations: (1) access to data, guaranteeing to users of digital platform their rights to access and use their own personal and non-personal data related to the respective digital identities; and (2) transparency, obliging digital operators to ensure the transparent use of the information they hold on users (including data related to their digital identities).

Q 2. How is self-determination exercised and protected in the metaverse in your jurisdiction?

Self-determination is a key principle and objective in regard to the development and use of digital identities in the metaverse in the EU region. Self-determination refers to the ability of users to control their own online identity and data, as well as to choose how, when and with whom they interact in the virtual environment. There may be several ways in which self-determination is exercised and protected in the metaverse, such as:

- the European digital identity wallet, which is designed to give users full control over their personal data and the sharing of identity attributes, in accordance with the GDPR and other data protection rules. The wallet also allows users to choose the appearance and features of their digital avatar, and to limit the disclosure of identity data to that which is strictly necessary for the provision of a service;
- the Digital Services Act, which aims to protect users from illegal and harmful content and practices in the online environment, and to ensure the transparency and accountability of online platforms. The Act also prohibits online platforms from using dark patterns or coercive choice architecture, which may manipulate users' decisions or preferences;

19 Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

- the AI Act, which proposes a human-centric approach to artificial intelligence (AI) and prohibits the use of subliminal, manipulative or exploitative techniques that may affect users' behaviour, choices or emotions in the metaverse. The Act also sets out rules for the use of biometric identification and categorisation systems, which may affect users' privacy and dignity in the virtual world.

Q 3. How is the role of intermediary ID providers regulated in your jurisdiction? What are some of their main obligations?

The role of intermediary ID providers, which are entities that provide the means of electronic identification or electronic attestations of attributes to users or parties relying on such information, is regulated in the EU region by the eIDAS Regulation[20] and its proposed amendment.[21] According to these regulations, some of their main obligations are:

- to comply with the technical and security requirements set out in the eIDAS Regulation and its implementing acts, as well as with the relevant cybersecurity and data protection rules;
- to obtain certification or conformity assessments for their means of electronic identification or electronic attestations of attributes, and to notify the competent authorities of their intention to provide such services;
- to cooperate with the competent authorities and other providers in regard to the interoperability, supervision and monitoring of their services, and to report any security breaches or incidents that may affect their services; and
- to respect the rights and interests of the users and the parties relying on such information, and to provide them with clear and transparent information about their services, including the level of assurance, the identity data and attributes involved, and the terms and conditions of use.

Q 4. Are there any upcoming policies, strategies or regulations that will impact the digital identify and authentication process in the metaverse?

The European Commission has proposed a regulation to amend the eIDAS Regulation and establish a framework for a European digital identity, which would provide users with secure and user-controlled digital wallets that can be used across borders to access public and private services. The proposal also aims to create a new qualified trust service for the attestation of attributes, such as personal or professional qualifications, that can be offered, shared and exchanged across borders in a way that offers full security, adequate data protection and has legal effect.

20 Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

21 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity.

AI in the metaverse

Eric Wagner *Gleiss Lutz, Stuttgart*
Marc Ruttloff *Gleiss Litz, Stuttgart*

Q 1. Are there any policies, strategies or regulations applicable to AI or the use of AI in the metaverse in your jurisdiction?

As AI and the metaverse offer not only opportunities but also risks, they are product sectors that require regulation. Due to the topicality of the subject matter, there is currently no regulatory framework either in Germany or in Europe, although this will soon change. The European Parliament adopted the current version of the AI Regulation on 13 March 2024 and the EU is expected to adopt the AI Regulation in mid-2024. It includes provisions which will not only regulate the marketing, commissioning and use of AI systems, but also the metaverse, although this is not clear from any part of the draft regulation. However, based on interpretation and legislative materials, it can now be said that the metaverse is not explicitly excluded from the scope of application: the European Commission and the European Parliament agree that the metaverse and the products in the metaverse are covered by the AI Regulation.[22] In addition, the European Commission expressly intends not to adopt any regulatory measures specifically aimed at the metaverse, as it considers the existing legal framework to be sufficient.[23] Nevertheless, on 17 January 2024, the European Parliament expressed its opinion on the existing regulatory framework and called on the European Commission to adopt new regulations specifically geared towards the metaverse, if necessary.[24] However, without an explicit regulation, it remains completely unclear, for example, when a virtual product falls within scope of the compliance requirements of the AI Regulation, to what extent the administrative structures provided for in the AI Regulation are transferable to virtual spaces, or how the obligations and sanctions are to be enforced.[25]

Particularly in view of the rapid technical developments in the field of the metaverse and its constantly growing importance, it is, therefore, too short-sighted to consider the existing legal framework to be sufficient. An entirely new world is emerging, not only in fact but also in law, which harbours a multitude of dangers that require regulation. The examples cited show that evaluations of a regulation that was created for the 'real world' cannot necessarily be transferred to the metaverse.[26] For this reason, it cannot be ruled out, and from a legal perspective it is even more advisable, that Union law must be further amended in order to take sufficient account of the special features of virtual spaces.[27] There is, however, an Artificial Intelligence Strategy issued by the German government in 2018, which was updated in 2020 and is intended as a political framework to strengthen German competitiveness and specify funding measures with regard to artificial intelligence (AI).[28]

22 Marc Ruttloff, Lisa Kappler, Hannah Bug in Eric Wagner, Moritz Holm-Hadulla and Marc Ruttloff, *Metaverse und Recht* (C.H. Beck, 2023), s 7 Rn. 413; Marc Ruttloff, Eric Wagner and Jana Schulz-Kuhnt, *Product Compliance im Metaverse* (BB 2022), p 499f; European Commission, *Thierry Breton's answer to the parliamentary question* E-000656/2022 (P-000656/2022, 1June 2022); European Parliament, *Briefing, Metaverse: Opportunities, risks and policy implications* (E 733.557, June 2022), 7.

23 European Commission, *Thierry Breton's answer to the parliamentary question* E-000656/2022 (P-000656/2022, 1 June 2022); Ruttloff, Kappler and Bug in Wagner, Holm-Hadulla and Ruttloff, *Metaverse und Recht* (2023), s 7 Rn. 413; Ruttloff, Wagner and Schulz-Kuhnt, *Product Compliance im Metaverse* (2022), pp 2500, 2505.

24 European Commission, Web 4.0 *und virtuelle Welten: Kommission stellt EU-Strategie vor – Europäische Kommission (Web 4.0 and virtual worlds: Commission presents EU strategy** *Publisher's translation) (11 July 2023), https://germany.representation.ec.europa.eu/news/web-40-und-virtuelle-welten-kommission-stellt-eu-strategie-vor-2023-07-11_de, accessed 7 March 2022; European Parliament, *Policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues* (P9_TA(2024)0029) (2019–2024), www.europarl.europa.eu/doceo/document/TA-9-2024-0029_EN.pdf, accessed 8 March 2024.

25 Ruttloff, Kappler and Bug in Wagner, Holm-Hadulla and Ruttloff, *Metaverse und Recht* (2023), s 7 Rn. 414; Ruttloff, Wagner and Schulz-Kuhnt, *Product Compliance im Metaverse* (2022), 2500.

26 Ruttloff, Wagner and Schulz-Kuhnt, *Product Compliance im Metaverse* (2022), 2505; Mario Martini and Jonas Botta, *Der Staat und das Metaversum* (MMR, 2023), 887.

27 Ruttloff, Wagner and Schulz-Kuhnt, *Product Compliance im Metaverse* (2022), p 2505; Martini and Botta, *Der Staat und das Metaversum* (2023), 887; Markus Kaulartz, Alexander Schmid and Felix Müller-Eising, *Das Metaverse – eine rechtliche Einführung* (Rdi, 2022), 521.

28 German Government, *Federal Government's Artificial Intelligence Strategy – Update 2020* (2 December 2020), www.bundesregierung.de/breg-de/service/publikationen/strategie-kuenstliche-intelligenz-der-bundesregierung-fortschreibung-2020-1824642, accessed on 5 March 2024.

2. How is transparency and accountability of AI ensured in your jurisdiction?

At present, there are no specific regulations in this regard.[29] However, the AI Regulation will subdivide AI systems into different categories based on their objective riskiness, all of which define different duty regimes and compliance requirements, including transparency and accountability obligations, which in turn consist of numerous information, documentation and notification obligations. The extent and scope of these obligations therefore depends on the categorisation of the AI system and cannot be described in general terms.

However, Article 50 of the AI Regulation standardises a general transparency obligation for AI systems of all kinds, which mainly imposes labelling obligations on providers and users in regard to AI-generated content to avoid the distortion of reality. In the event of a violation, Article 99 of the AI Regulation imposes high fines, while the European and, above all, national (supervisory) authorities, are given numerous powers in order to take administrative measures throughout the entire body of regulations, but in particular in Article 79 of the AI Regulation, ranging from the imposition of conditions and temporary interruptions to operations to a permanent ban on AI systems.

While there is discussion about how AI can be used in criminal (procedural) law,[30] there is still no specific AI criminal law, so from a criminal law perspective, existing norms must be used. The same applies to German civil law, whose existing legal obligations, product liability and tort law structures are, however, not completely sufficient in regard to their application to AI inconsistencies and may require a makeover.[31] The European Commission has responded to this by submitting both a proposal for a separate legal act on non-contractual liability for AI and a proposal to revise the Product Liability Directive.[32]

3. How is algorithmic bias mitigated in your jurisdiction? Are there any policies, strategies or regulations aiming to promote fairness and non-discrimination?

Preventing the development and use of discriminatory AI algorithms, which are unacceptable under constitutional law, represents a major challenge. In addition to the existing anti-discrimination structures under German and European law, the AI Regulation, which is based on an anti-discriminatory model, also aims to address this issue. In Article 5, it therefore stipulates prohibited AI practices, which primarily include biometric classification and identification systems, whereby the risks of discrimination inherent to a person's appearance are nipped in the bud.

In addition, Annex III of the AI Regulation lists areas of AI use that are problematic in terms of fundamental rights and makes the corresponding AI systems subject to the high-risk regulation regime, which provides for increased discrimination protection mechanisms. In particular, discrimination risks should be researched, recognised and documented at an early stage. The market surveillance authorities, which of course also protect fundamental rights, can request access to this documentation, in accordance with Article 64 of the AI Regulation. Otherwise, the general German and European anti-discrimination laws, such as the German General Equal Treatment Act, with its provisions on protection against discrimination in civil law transactions, are of course applicable.

4. What is the intellectual property law treatment of AI-generated content used in the metaverse in your jurisdiction? Who are the rightsholders of that content?

Since the metaverse is not a legal vacuum, it goes without saying that immaterial goods regulations also apply in the metaverse, provided that — as the territoriality principle presupposes — there is a sufficient domestic connection, which

29 Deutscher Bundestag, Wissenschaftliche Dienste, *Regulierung von künstlicher Intelligenz in Deutschland (Regulation of Artificial Intelligence** *Publisher's translation) (Sachstand WD 5-3000 – 001/23; 19 January 2023), 4.

30 European Parliament (Legislative Observatory), *Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2020/2016(INI)).

31 Hans Steege and Kuuya Chibanguza, *Metaverse Rechtshandbuch* (Nomos 2023), 178.

32 European Commission, *Proposal for a directive of the European Parliament and of the Council on liability for defective products* (COM (2022) 495 final (28 September 2022)).

could lead to application problems in the metaverse.[33] German copyright law does not recognise the transferability of copyrights, so even if the terms of use provide for this, no (copyright) rights to the AI output can be transferred to the user.[34] This is precisely why copyrights must be observed, especially in the metaverse. Such a transfer could – if at all – only be reinterpreted as the granting of rights of use.[35] In addition, the AI output itself cannot even be considered a work worthy of copyright protection, as copyright law is based on an anthropocentric model that only grants human beings the status of creator.[36] The European Court of Justice (ECJ) demands that the author must make the creative decisions, which is not the case when using an AI system.[37] In the case of a pure reproduction or translation, the copyrights of the original author continue to exist and the AI-generated content cannot be used freely.[38] Copyrights may also continue to exist in the case of redesigns, depending on how much of the original is hidden in the AI-generated content, so that this content may not be freely usable either.[39] However, copyright infringement is very unlikely in the case of informative specialist content, as the ECJ imposes very strict requirements in this field. The text content is determined by objective information, which is why the author 'could not express his creative spirit in an original way'.[40] The AI Regulation also addresses copyright law and makes it clear in many places that the regulations are without prejudice to copyright law.[41]

Q 5. Which stakeholders are liable for any damages caused to third parties due to the use of AI in the metaverse? What sanctions (civil, criminal, administrative) may apply in case of infringement?

At present, AI liability issues still have to be assessed according to the law of obligations, tort and product liability law, as there is no corresponding, more specific set of regulations.[42] However, due to the autonomy and the associated autonomy risk, whose bearer cannot always be easily determined, there are significant attribution problems.

However, in order to make the most of the economic and social benefits of AI and to promote digital economic change, the European Commission submitted a proposal for a directive on 28 September 2022 to adapt the rules on non-contractual civil liability to AI.[43] That applies to non-contractual fault-based civil claims for damages caused by an AI system and addresses the special characteristics of certain AI systems.

The proposed directive is based on a rebuttable presumption of fault at the expense of the provider, a person associated with the provider or the deployer and gives the injured parties a (subsidiary) right of disclosure with regard to evidence, as they must sufficiently prove the plausibility of a claim for damages by presenting facts and evidence. If the defendant fails to comply with its duty of disclosure ordered by the court, the court will presume that it is at fault. If this is the case and the plaintiff can prove a breach of duty and a causality fulfilling liability, or if the latter can be assumed without error of judgment, the court assumes that the defendant is at fault and, in this context, refutably presumes a causality between the defendant's fault and the result produced by the AI system.

There are separate provisions for high-risk AI systems that simplify the evidence requirements. The AI Regulation has undergone immense extensions of system-defining dimensions that could not be taken into account on 28 September 2022, in regard to the adoption of the AI Liability Directive.. Before the AI Liability Directive is adopted, it is expected that it will be adapted in regard to the AI Regulation. In connection with the AI Regulation and the AI Liability Directive, a

33 Stefan Weidert, Alexander Molle and Victoria von Werder in Wagner, Holm-Hadulla and Ruttloff, *Metaverse und Recht* (2023), s 6 Rn. 338 ff, s 7 Rn. 407; Kaulartz, Schmid and Müller-Eising, *Das Metaverse – eine rechtliche Einführung* (2022), 531; Sven Hetmank and Anne Lauber-Rönsberg in Hans Steege and Kuuya Chibanguza, *Metaverse Rechtshandbuch* (Nomos, 2023), 235.
34 Vgl. s 29 Abs. 1 UrhG.
35 Marcus von Welser, *ChatGPT und Urheberrecht* (GRUR-Prax, 2023), 57; LG München I, Urteil vom 14.05.2012–21 O 14914/09, BeckRS 2012, 13691.
36 Vgl. s 2 Abs. 2 UrhG; Anne Lauber-Rönsberg, *Autonome 'Schöpfung' – Urheberschaft und Schutzfähigkeit* (GRUR, 2019), 244.
37 EuGH (Große Kammer), Urt. v 29.7.2019–C-469/17, Rn. 25; Weidert, Molle and von Werder in Wagner, Holm-Hadulla and Ruttloff, *Metaverse und Recht* (2023), s 6 Rn. 387.
38 von Welser, *ChatGPT und Urheberrecht* (2023), 58.
39 *Ibid.*
40 EuGH (Vierte Kammer), Urteil vom 16. 7. 2009 - C-5/08, Rn. 48.
41 Vgl. recital No 28a, 57d, 83; Arts 25(5), 52b(5), 53(1)(b), 78(1)(a), Annex VII point 4.5 AI-Act.
42 Deutscher Bundestag, Wissenschaftliche Dienste, *Regulierung von künstlicher Intelligenz in Deutschland* (Sachstand WD 5-3000 – 001/23; 19 January 2023), 4.
43 Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (Directive on AI liability), COM (2022) 496 final, 2022/0303(COD), 29 September 2022.

directive on liability for defective products was also proposed, which is intended to adapt product liability law.[44] However, the AI Liability Directive does not create its own basis for claims and does not lay down any general provisions, such as which damages are eligible for compensation or what requirements must be met in terms of proof. [45] All of this is the task of the national legislators.

Article 1(4) of the draft Directive provides that Member States may adopt or maintain provisions that further facilitate the enforcement of claims for damages by the injured party and, thus, opens the door for Member States to structure liability as strict liability regardless of fault.[46] It, therefore, remains to be seen which liability systems national legislators will opt for when implementing the directive. Once the AI Regulation becomes applicable, its provisions will also play a significant role in this regard and, above all, will provide the competent authorities with special administrative sanctions. If the relevant facts are fulfilled, German criminal law will also apply.

On 17 January 2024, the European Parliament dealt with the Web 4.0 initiative and virtual worlds and called on the European Commission to review the effectiveness of existing legislation on a permanent basis and to adopt new legislation if necessary.[47] That is why the metaverse may soon have its own liability rules if the AI Liability Directive is unable to achieve the desired effects in regard to the metaverse.

Q 6. Are there any upcoming policies, strategies or regulations that will impact AI in your jurisdiction?

As described above, the AI Regulation, the AI Liability Directive and the supplement to the Product Liability Directive are currently being developed at European level with regard to AI. The EU Parliament adopted the current version of the AI Regulation on 13 March 2024.

There are still no specific AI regulations at national level, which is why we are eagerly awaiting the adoption of EU legislation while applying the existing general regulations.[48] There is, however, an 'Artificial Intelligence Strategy' from the German Government from 2018, which was updated in 2020 and is intended as a political framework to strengthen German competitiveness and specify funding measures with regard to AI.[49] This strategy will probably be adapted and updated over time.

44 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM (2022) 495 final, 2022/0302(COD), 29 September 2022.
45 Dirk Staudenmayer, *Haftung für Künstliche Intelligenz* (NJW, 2023), 895.
46 Vgl. recital No 11 of the draft directive.
47 European Commission, *Web 4.0 und virtuelle Welten: Kommission stellt EU-Strategie vor – Europäische Kommission* (11 July 2023); European Parliament, *Policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues* (P9_TA(2024)0029) (2019–2024).
48 Deutscher Bundestag, Wissenschaftliche Dienste, Regulierung von künstlicher Intelligenz in Deutschland (Sachstand WD 5- 3000 – 001/23; 19 January 2023), 4.
49 German Government, *Federal Government's Artificial Intelligence Strategy – Update 2020* (2 December 2020).

Human rights, accessibility and digital ethics

Daniela De Pasquale *Ughi e Nunziante, Milan*
Timoteo Bucci *Ughi e Nunziante, Milan*

Q 1. Are there any human rights, accessibility and digital ethics strategies, polices or regulations applicable to the metaverse in your jurisdiction?

Whereas no regulations and policies addressing the metaverse specifically have been adopted yet at EU level, human rights, accessibility and digital ethics issues are already dealt with by various pieces of legislation, which may apply to the metaverse environment on a case-by-case basis.

Firstly, the protection of the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union has been complemented by a set of 'digital rights and principles', an inter-institutional declaration that sets out a framework of reference for the digital enforcement of such rights, taking into account the developments throughout the digital decade. [50] [51] [52]

Within such framework, the following pieces of legislation, each within its own remit, may apply in connection with different aspects of the development of the metaverse:[53]

- the GDPR, concerning the processing of personal data in virtual worlds;[54]
- the General Product Safety Regulation (GPSR)[55] and the Unfair Commercial Practices Directive, aimed at ensuring consumer protection with respect to product safety and also aiming to protect consumers against misleading and aggressive commercial practices;[56]
- the Digital Services Act (DSA), which aims to create a safe, predictable and trusted online environment, applicable to intermediary digital services offered to recipients (such as metaverse users) established or located in the EU;[57]
- the Digital Markets Act, which introduces a comprehensive set of rules for entities acting as gatekeepers of core platform services;[58]

50 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
51 I. Hupont Torres, V. Charisi, G. De Prato, K. Pogorzelska, D. Schade, A. Kotsev, M. Sobolewski, N. Duch Brown, E. Calza, C. Dunker, F. Di Girolamo, M. Bellia, J. Hledik, I. Nai Fovino and M. Vespe, *Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU* (Luxembourg: Publications Office of the European Union, 2023), https://op.europa.eu/en/publication-detail/-/publication/775e6eec-16f5-11ee-806b-01aa75ed71a1/language-en accessed 20 June 2024.
52 European Declaration on Digital Rights and Principles for the Digital Decade, COM/2022/28 final.
53 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition, Strasbourg, 11 July 2023, COM/2023/442 final.
54 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.
55 Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) 1025/2012 and Directive (EU) 2020/1828 and repealing Directive 2001/95/EC and Directive 87/357/EEC [2023] OJ L135/1.
56 Directive 2005/29 concerning unfair business-to-consumer commercial practices in the internal market and amending Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC and Regulation 2006/2004 [2005] OJ L149/22.
57 Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC [2023] OJ L277/1.
58 Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/1.

- the Data Act, aimed at giving users control over the data generated by their connected devices;[59]
- the Artificial Intelligence Act, which addresses the risks associated with artificial intelligence systems ('AI Act'),[60] complemented by the proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence ('AI Liability Directive'); and [61]
- the proposed regulation on European digital identity, which will provide users with control over their digital identities. [62]

Among the above pieces of legislation, a key role in shaping the rules applying to the metaverse — in addition to the GDPR and AI Act — will be played by the Digital Services Act.

Most notably, the DSA imposes upon providers of very large platforms (ie, with more than 45 million users) obligations on the assessment and mitigation of systemic risks stemming from the design or functioning of their services and related systems.[63] Among such systemic risks, the DSA prominently mentions any actual foreseeable negative effects in relation to the protection of public health, non-discrimination, freedom of expression, freedom of information and in relation to minors.

The DSA also provides for obligations concerning content moderation and the takedown of illegal content from the relevant platforms upon knowledge of its presence, as well as on the notification of suspicions of serious criminal offences to the competent authorities.[64]

Infringements of the provisions in the DSA are sanctionable with fines amounting up to six per cent of the annual for the preceding financial year of the service provider involved.

In the event of a failure to remove timely adopt the corrective measures imposed by the competent authorities in a timely manner, service providers may also be subject to other negative consequences, such as additional periodic penalty payments and — in the most serious cases — temporary restrictions on access to the online interface on which the infringements occurred.

In future, the DSA may be complemented by further regulations and policies addressing specific issues, topics and technologies concerning the digital and online environment, as several studies and strategic documents published by the European Council, the European Parliament and the European Commission expressly encourage the promotion of legislative initiatives and policies in this regard, including in relation to the metaverse.

Q 2. Considering the various health risks associated with the metaverse and related technologies, are there any strategies, policies and regulations in your jurisdiction that aim to protect public health

The physical and mental health risks associated with the metaverse and related technologies are outlined in several studies published by the EU institutions over the past few years.

In particular, a 2022 briefing published by the European Parliament's Research Service (the 'European Parliament Metaverse Briefing') notes that the metaverse – if used to excess – can cause mental health problems (such as loneliness) and reduce physical activity, leading to an increase in obesity and other physical health problems. It further adds that, as people are distracted while using the metaverse, harmful accidents can happen either in real life to the person in the metaverse or to the persons or things (such as furniture) around them.[65]

Another 2023 study, published by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (the 'European Parliament Metaverse Study'), delves specifically into the phenomenon known as cybersickness.

59 Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L.
60 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.
61 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM/2022/496 final.
62 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.
63 Digital Services Act, Arts 4 para 1, lett (i); 33; 34; 45.
64 Digital Services Act, Arts 9; 6; 18.
65 *Metaverse – Opportunities, risks and policy implications* (European Parliamentary Research Service, June 2022).

As in traditional 360-degree virtual reality (VR) experiences translational movement occurring in the real world is not reflected in the virtual world, the actual self-motion information used is not confirmed by matching visual and vestibular cues; this may trigger symptoms typically associated with motion sickness, including nausea, disorientation, oculomotor disturbances, drowsiness (so-called 'sopite syndrome') and other types of discomfort.[66]

While the currently applicable legal framework does not include provisions aimed at tackling health risks in the metaverse specifically, certain physical tech products, such as VR headsets, which are in some instances required to enter the metaverse, are already covered by the recently issued General Product Safety Regulation (GPSR), which provides for several product safety requirements, as well as record-keeping and information obligations, addressed to product manufacturers, importers and distributors. The rules on the penalties applicable for violation of the GPSR's provisions were due to be laid down by Member States and notified to the European Commission by 13 December 2024.

As stated in the previous paragraph, the DSA will also be applicable to public health concerns as a systemic risk: the DSA acknowledges the risks associated with serious negative consequences for the physical and mental wellbeing of individuals, which providers of very large platforms and search engines are required to assess and mitigate in regard to the provision of their services.

In the near future, it is likely that EU institutions will issue new policies and regulations addressing the risks to health posed by the metaverse in the upcoming years, as the European Commission has announced its intention to support research on the impact of virtual worlds on people's physical and mental health and wellbeing, in line with a comprehensive approach to mental health.[67]

Q 3. Considering the various discrimination risks associated with the metaverse and related technologies, are there any strategies, policies or regulations in your jurisdiction aimed at ensuring non-discrimination?

A 2023 report, published by the Parliamentary Assembly of the Council of Europe (the 'EU Council Metaverse Report'), addresses discrimination based on race, gender, sexual orientation, religious beliefs and age as one of the main concerns posed by the metaverse, as all such characteristics may negatively impact access to education, work opportunities, political life and services for some groups of people.[68]

Such a view is consistent with the inclusion of any actual or foreseeable negative effects on human dignity and non-discrimination among the systemic risks addressed by the DSA.

With a focus on the digital world, both the GDPR and the AI Act include provisions requiring the involvement of human intervention to some degree, or a clear understanding of the functioning of algorithms, in regard to processes whereby automated or machine-based decisions may impact the rights of individuals. The purpose of such provisions is to prevent, insofar as possible, any discriminatory effect upon individuals.

In regard to a wider, not exclusively digital scope further EU policies may apply to the metaverse environment with respect to specific kinds of discrimination, namely Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services, which applies to all persons who provide goods and services being offered outside the area of private and family life (either in the public and private sectors, including public bodies); and Council Framework Decision 2008/913/JHA, which sets out that each Member State shall take the measures necessary to ensure that offences concerning racism and xenophobia are prosecuted as criminal law offences.[69] [70]

Both pieces of legislation delegate to each Member State the determination of the penalties applicable to infringements of the domestic provisions adopted to implement them in that jurisdiction's national legal framework. A further proposal for a council directive on implementing the principle of equal treatment between persons irrespective of religion or belief,

66 *Metaverse*, PE 751.222 (Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, Directorate-General for Internal Policies, June 2023).
67 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a comprehensive approach to mental health, COM/2023/298 final.
68 *Risks and opportunities of the metaverse,* AS/Cult (Parliamentary Assembly of the Council of Europe, 2023).
69 Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L373/37.
70 Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law [2008] OJ L328/55.

disability, age or sexual orientation was published in 2008, but has not yet been adopted due to a lack of agreement between the Member States.[71]

Q 4. Considering the risks to freedom of expression and censorship associated with the metaverse, are there any strategies, policies or regulations in your jurisdiction aiming to mitigate them/promote freedom of expression and non-censorship?

Whereas the DSA expressly includes any actual or foreseeable negative effects for the exercise of fundamental rights, including freedom of expression and freedom and pluralism of the media, among the systemic risks that every very large platform provider must take into account, many commentators have remarked that a serious threat to the fundamental rights at issue might lie in the obligations on content moderation provided by the DSA itself.[72, 73]

In particular, as a result of the duty imposed on platform providers to set up content moderation mechanisms and procedures, although shaped by the provision of specific mandatory features (including the need for human oversight), platforms are ultimately vested with substantial censorship powers that had traditionally been a prerogative of public authorities, thereby epitomising the final step of a phenomenon that has been labelled in the legal literature as the 'privatisation of censorship'.[74]

In establishing a consistent approach, the European Parliament Metaverse Study observes that the decisions by some companies to develop a self-regulation approach to metaverse content moderation has been met with scepticism and invites policymakers to take further initiatives, so that online platforms and law enforcement authorities are better able to exercise their content moderation and removal duties.

It is worth mentioning that the issue of censorship was addressed by the emergency resolution adopted by the European Parliament in 2022 on the Russian aggression against Ukraine, which set forth a number of restrictive measures in view of Russia's actions against Ukraine, including the prohibition of broadcasting content by the legal persons, entities and bodies listed in Annex IX to the resolution.[75] The resolution was challenged by a French media broadcaster before the CJEU for alleged breach of the rights of defence, freedom of expression and information, but the resolution was upheld by the CJEU.[76]

Among the new pieces of legislation that will likely be adopted in the coming years, the proposed European media freedom act – currently at the trilogue stage – provides for rights and obligations of media service providers that will likely apply to the metaverse.[77]

The issue of censorship versus freedom of speech is also one of the topics addressed in the 2023 EU initiative on Web 4.0 and virtual worlds: a headstart in the next technological transition, according to which the European commission purports – among other things – to launch a structured approach to monitoring the development of virtual worlds across all industrial ecosystems, together with Member States and stakeholders.[78]

71 Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation SEC(2008) 2180; SEC(2008) 2181/*COM/2008/0426 final – CNS 2008/0140.

72 Ottavio Grandinetti, 'Le Piattaforme digitali come "poteri privati" e la censura online' (2022) 1 *Rivista Italiana di Informatica e Diritto*.

73 Andrea Palumbo and Jacopo Piemonte, 'Delega di funzioni regolamentari e lotta ai rischi sistemici causati dalla disinformazione nel Digital Services Act: quali rischi per la libertà di espressione?' (2024) 1 *Media Laws*.

74 Julie Adler, 'The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship' (2011) 20(1) *The Journal of Law and Policy*.

75 Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2022] OJ L65/5; Regulation (EU) 2022/350 amending Regulation (EU) 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2022] OJ L65/1.

76 *RT France v Council* (T-125/22) CJEU, Judgement of the General Court (Grand Chamber).

77 Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU, EU Commission COM/2022/457 final.

78 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition* EU Commission COM/2023/442 final.

Q 5. Considering the risks of misinformation and the risks associated with fake news and deep fakes in the metaverse, are there any strategies, policies or regulations in your jurisdiction aiming to mitigate them/promote freedom of expression and non-censorship?

The European Parliament Metaverse Study identifies false information and manipulation as key concerns in regard to the metaverse, in particular in connection with technologies that enable a perfect reproduction of the facial features and voice of any individual, such as deepfakes.

All such issues are covered by the risk assessment and mitigation obligations provided for by the DSA, as well as being subject to the content moderation activity imposed on platforms.

Moreover, Article 25 of the DSA expressly provides that providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their services or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.

Further applicable provisions include, from an advertising point of view, the Unfair Commercial Practices Directive, which provides the consumer with information that is false and untruthful, or in any way deceives or is likely to deceive the average consumer in connection to certain product characteristics, shall be regarded as an unfair commercial practice and subject to the penalties set forth in the provisions adopted by each Member State in the transposition of such Directive.[79]

Furthermore, the majority of the key stakeholders are subscribers to a voluntary adhesion initiative named the 'Code of Practice Against Disinformation', first published in 2018 and reinforced in 2022 with a 'strengthened' version.[80]

The Code of Practice Against Disinformation aims to combat misinformation, disinformation and undue influence in the information space by providing a list of commitments concerning several aspects including scrutiny of advertisement placements, demonetisation of disinformation and tackling advertising containing disinformation, as well as further commitments including monitoring of political advertisements, civil society efforts, collaboration between subscribers, integrity and safe design of services, transparency, user empowerment and enhancing media literacy.

Q 6. Are there any strategies, policies or regulations in your jurisdiction aiming to ensure accessibility and inclusion in the metaverse? How are they enforced?

The European Parliament Metaverse Study highlights that although, in principle, the metaverse is open to all, in practice, many people could face problems in regard to gaining access, ranging from a lack of digital skills, as a result of poor digital literacy, to not having suitable broadband or hardware, due to the high cost of the equipment that is necessary in some instances.

Moreover, the European Parliament Metaverse Study notes that the DSA has faced criticism for not including accessibility requirements for persons with disabilities in its mandatory provisions, which has only been addressed in the encouragement by the European Commission to draw up codes of conduct to address their particular needs.[81]

Formatting incorrect fall within the scope of applicability of the European Accessibility Act, which will apply to services provided to consumers after 28 June 2024 and sets forth accessibility requirements for economic operators to comply with during the design of their services.[82]

The European Accessibility Act entrusts Member States with determination of the penalties for non-compliance with its provisions, which shall be accompanied by effective remedial action in the case of non-compliance by the economic operator at fault.

79 Directive 2005/29/EC concerning unfair business to consumer commercial practices in the internal market and amending Directive 84/450 EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC and Regulation (EC) 2006/2004 [2005] OJ L149/22.
80 European Commission, 2022 Strengthened Code of Practice against misinformation (16 June 2022), https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation, accessed 20 June 2024.
81 Digital Services Act, Art 47.
82 Directive (EU) 2019/882 on the accessibility requirements for products and services [2019] OJ L151/70.

With respect to future perspectives, in 2021 the EU Commission published a communication headed *Union of Equality: Strategy for the Rights of Persons with Disabilities 2021–2030*, which addresses the topic of accessibility in several policy areas with the purpose of reducing discrimination, inequalities and supporting persons with disabilities to fully enjoy their human rights and fundamental freedoms.[83] As equal digital accessibility is a key principle of such communication, future regulations stemming from it may also cover the metaverse.

Q 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring protection of minors in the metaverse?

Due to their increased vulnerability in online environments, the protection of minors in the metaverse is likely the most sensitive policy area in connection with the metaverse: among the risks that it implies for children, the EU Parliament Metaverse Briefing mentions abuse, harassment, bullying, racism and exposure to pornographic content.

Although no specific legal provisions addressing such risks in the metaverse have yet been adopted, many policies and regulations aimed at protecting the rights of children in several areas are already applicable to the metaverse environment.

The DSA, in addition to the express inclusion of any foreseeable negative impact on children protection among the systemic mentioned above, also imposes on providers of online platforms accessible to minors obligations to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors on their service, and prohibits interface advertisements based on profiling being served to recipients of the service who they believe with reasonable certainty to be minors.[84]

Directive (EU) 2010/13 concerning the provision of audio-visual media services, in order to protect children, imposes on video-sharing platforms the obligation to adopt parental controls and age verification systems, and to offer easy ways for users to rate, flag and report illegal or harmful content.[85]

Directive (EU) 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography covers prosecuting offenders, protecting victims and preventing offences, as well as blocking and taking down websites that host and distribute child sexual abuse material.[86]

The Unfair Commercial Practices Directive explicitly lists the direct encouragement of children to buy things or persuade their parents or other adults to buy advertised products for them among the prohibited aggressive commercial practices.

As for future perspectives, the enhancement of the protection of minors in the digital environment is the core objective of many strategic documents already issued by the EU institutions, including – most notably – the European Commission's 'New European strategy for a better internet for Kids' (BIK+).[87]

Among the new proposed legislative initiatives that aim to enhance the protection of children online, the European Commission published a regulatory proposal and should be lower case in 2022 laying down rules to prevent and combat child sexual abuse, which has been subject to strong criticism as it sets forth that in the event of suspected dissemination via chat of paedo-pornographic content, messaging service providers must undertake massive surveillance of the messages, videos and photos exchanged via their services.[88]

On a final note, at the EU–US Trade and Technology Council held on 30 and 31 May 2023, the EU and the US expressed their joint view that online platforms should take greater responsibility to ensure that their services contribute to an online

83 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Union of Equality: Strategy for the Rights of Persons with Disabilities 2021–2030, EU Commission COM/2021/101 final.
84 Digital Services Act, Art 28.
85 Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services [2010] OJ L95/1.
86 Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/1.
87 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*, EU Commission COM /2022/ 212 final.
88 Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, EU Commission COM/2022/209 final.

environment that protects, empowers and respects children and young people, and should take responsible action to address the impact of their services on the mental health and development of children and young people. [89]

Q 8. Are there any policies, strategies or regulations in your jurisdiction focused on ethics-by-design in the metaverse? How are these rules enforced?

The topic of ethics-by-design in connection with the metaverse is not currently addressed by specific regulations or policies, but several provisions of the DSA impose upon platform providers obligations that fit such a label, such as the ones concerning transparency, the adoption of measures and protection against misuse, online interface design and organisation, as well as – for very large platform providers – risk assessment and mitigation.

The EU Parliament Metaverse Study delves thoroughly into the ethical issues implied by the metaverse and proposes to adopt as a reference for building and managing the metaverse the European Parliament's work on ethical principles for artificial intelligence and the subsequent EU Commission's Ethics Guidelines for Trustworthy Artificial Intelligence.[90]

In this respect, the EU Parliament highlights that the metaverse – as well as artificial intelligence – is not just another product for consumers, but rather a tool of economic dominance which may also be used as a weapon or spyware. Therefore, European ethical values and fundamental principles of law need to regulate metaverse in these areas, so that EU can effectively protect individual rights of its citizens and its democracy. Hence, as a new platform for governance, the EU Parliament stresses that the metaverse can be built on the principles of universal fundamental rights, innovation and cooperation.

Q 9. Are there any upcoming policies, strategies and regulations that will impact human rights, accessibility and digital ethics requirements in your jurisdiction?

We have addressed this issue at the bottom of each respective answer.

89 Joint Statement EU–US Trade and Technology Council of 31 May 2023 in Lulea, Sweden.
90 High-Level Expert Group on Artificial Intelligence set up by the European Commission, Ethics Guidelines for Trustworthy AI, 2019.

Competition law

Albert Agustinoy *Cuatrecasas, Barcelona*

Q 1. Are there any competition strategies, policies or regulations applicable to the metaverse in your jurisdiction?

The metaverse is subject to general EU competition rules and regulations that apply to digital services, online platforms and intermediary services, such as the Digital Markets Act (DMA) and the Digital Services Act (DSA):

- the DMA aims to ensure contestable and fair markets in the digital sector by imposing obligations and prohibitions on gatekeepers, which are companies with a significant impact on the internal market, providing important gateways for business users to reach end users, and having an entrenched and durable position; and
- the DSA regulates digital services by establishing harmonised rules for a safe, predictable and trusted online environment in the EU, and applies to intermediary services offered to recipients within the EU, regardless of the location of the provider's establisment.

In addition, the European Parliament briefing on the Metaverse sets forth that ensuring fair interconnection and interoperability conditions for multiple devices and platforms should be one of the top priorities for any future regulatory development related to the metaverse. In that respect, the paper identifies potential threats of the implementation of the said conditions, such as lack of standardisation and interoperability, acquisitions by large companies of innovative nascent competitors to halt innovation or risks of monopolisation of future digital markets. With the aim of addressing these issues, the European Parliament has suggested considering the adoption of the following actions:

- amending merger regulation to minimise the above-mentioned risks, with updated tools and criteria;
- compliance with updated antitrust rules (which should be reviewed to guarantee the identification of competitive issues arising from these new digital markets); and
- regulating standards setting and interoperability, prioritising open metaverse standards rather than proprietary ones.

Q 2. Are there any strategies, policies, regulations or best practices on how to carry out an antitrust or competition risk assessment?

There are no specific strategies, policies, regulations or best practices on how to carry out an antitrust and competition risk assessment in regard to the metaverse in the EU. However, the European Commission has launched calls for contributions to gather feedback on competition in virtual worlds and generative AI, which are components of the metaverse ecosystem. The European Commission may also initiate market investigations to assess and designate gatekeepers under the DMA, or review agreements between digital market players and generative AI developers/providers under the EU Merger Regulation.

The main provisions of the EU competition rules are contained in Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), which prohibit anti-competitive agreements and abuse of dominant position, respectively. These rules are implemented by Council Regulation (EC) 1/2003,[91] which establishes a system of cooperation and enforcement between the European Commission and the national competition authorities and courts in the Member States. The sanctions for non-compliance with the EU competition rules may include fines up to 10 per cent of the total worldwide turnover for the preceding year for companies, or up to 30 per cent for associations of undertakings, as well as periodic penalty payments, structural or behavioural remedies, or damages actions.

91 Council Regulation (EC) 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1.

Q 3. What are the rules regarding market dominance and barriers to entry applicable to the metaverse in your jurisdiction?

The rules regarding market dominance and barriers to entry applicable to the metaverse in the EU are the same as those applicable to any other market or sector, and are based on Articles 101 and 102 of the TFEU, as well as the Digital Markets Act.

The main provisions of Article 102 of the TFEU prohibit any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it, which may affect trade between Member States and prevent the full realisation of the benefits of the Single Market. The assessment of dominance depends on various factors, such as the market shares, barriers to entry, countervailing buyer power and network effects. Abuse of a dominant position may take various forms, such as predatory pricing, refusal to deal, tying and bundling, discrimination or excessive pricing.

The European Commission and the national authorities can impose fines up to ten per cent of the worldwide turnover for the preceding financial year of the infringing undertaking, and periodic penalty payments of up to five per cent of the average daily turnover of the company to compel compliance. The national courts can also award damages to the victims of the infringement. Moreover, the European Commission has the power to impose behavioural or structural remedies on the dominant undertaking to restore effective competition.

The DMA complements Article 102 of the TFEU by identifying and regulating gatekeepers, which are considered to have a dominant position in the digital sector, and by prohibiting certain practices by gatekeepers that undermine contestability and fairness, such as combining personal data from different sources without consent, or preventing users from uninstalling pre-installed software or apps.

Q 4. Are there any specific gatekeepers' obligations applicable to the metaverse in your jurisdiction?

The Digital Markets Act introduces specific obligations for gatekeepers, which are undertakings that provide core platform services and meet certain criteria in terms of their impact, intermediation and durability in the EU. Core platform services include online intermediation services, online search engines, social networking services, video-sharing platform services, number-independent interpersonal communication services, operating systems, web browsers, virtual assistants, cloud computing services and online advertising services. The metaverse may involve some or all of these services, depending on its features and functionalities. These gatekeepers are subject to prohibitions and obligations that aim to prevent unfair practices and ensure fair and contestable markets, such as: (1) restrictions on data processing and combining certain data without consent; (2) fairness in regard to commercial conditions and access; (3) the ability for business users to promote offers and conclude contracts with end users; (4) a prohibition on restricting users from raising non-compliance issues; and (5) a requirement to provide advertisers and publishers with access to performance measurement tools and the necessary data.

The European Commission monitors the compliance of gatekeepers and can impose fines up to ten per cent of the worldwide turnover for non-compliance, up to 20 per cent for repeated infringements and periodic penalty payments for non-compliance with interim measures or commitments. The European Commission can also investigate and designate gatekeepers, assess systematic non-compliance and examine new services and practices.

Q 5. Are there any competition strategies, policies and regulations in your jurisdiction related to the metaverse which aim to promote standardisation and access to fair and non-discriminatory licences?

The EU competition rules aim to promote standardisation and access to fair and non-discriminatory licences, as long as they do not restrict or distort competition in the internal market.

The Commission has issued guidelines on the application of Article 101 of the TFEU to horizontal cooperation agreements,[92] which includes agreements on standardisation. The guidelines set out the conditions and criteria for assessing the compatibility of standardisation agreements with Article 101 of the TFEU, such as the nature and scope of the standard, the participation and transparency of the standard-setting process, access to the standard and the essential patents and the safeguards against anti-competitive effects.

The European Commission has also issued guidelines on the application of Article 101 of the TFEU to technology transfer agreements,[93] which includes agreements on licensing. The guidelines provide a framework for assessing the compatibility of technology transfer agreements with Article 101 of the TFEU, such as the market power of the parties, the scope and duration of the agreement, the restraints on competition, and the efficiencies and benefits of the agreement. The European Commission has also adopted a block exemption regulation for technology transfer agreements, which exempts certain categories of agreements from the prohibition in Article 101 of the TFEU, subject to certain conditions and limitations.

Q 6. Are there any competition strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote interoperability in the metaverse?

One of the obligations for online platforms provided for in the DMA is to ensure interoperability of ancillary services, such as identification, payment or advertising services, with other online platforms, unless this would undermine the security or integrity of the service. Another obligation for very large online platforms and search engines is to provide access to and interoperability with their online interface, operating system or hardware or software features, to third-party providers of ancillary services or end users, under fair, reasonable, and non-discriminatory conditions.

Similarly, the Data Act aims to remove barriers to a well-functioning internal market for data. It applies to data sharing and data processing services, and establishes essential requirements for interoperability of data, data sharing mechanisms, services and Common European Data Spaces. These requirements include descriptions of dataset content, data structures, technical means to access data and interoperability of tools for automating data sharing agreements. The regulation also sets essential requirements for smart contracts executing data sharing agreements, such as robustness, safe termination, data archiving, access control and consistency with data sharing agreements.

Moreover, one of the actions provided for in the European Commission's Communication on Virtual Worlds is to foster global governance of virtual worlds, which will address interoperability and content practices, among other issues.

Q 7. Are there any upcoming policies, strategies or regulations that will impact competition in your jurisdiction?

The European Commission has published two calls for contributions on competition in virtual worlds and generative AI, which are technologies that could influence market dynamics and consumer behaviour in the metaverse.

The European Commission is also investigating agreements and investments between digital market players and generative AI developers/providers, such as Microsoft's investment in OpenAI, to check whether they are reviewable under the EU Merger Regulation.

92 *Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreement* (European Commission, 21 July 2023).

93 *Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements* (European Commission, 28 March 2014).

Digital transactions and ownership

Magda Cocco *Vieira de Almeida, Lisbon*
Iakovina Kindylidi *Vieira de Almeida, Lisbon*

Q 1. Are there any relevant policies, strategies or regulations applicable to tokens, non-fungible tokens (NFTs) and digital assets in the metaverse in your jurisdiction?

In the EU region, there are no specific or comprehensive policies, strategies or regulations that apply exclusively to tokens, NFTs and digital assets in the metaverse.

In relation to crypto assets, Regulation (EU) 2023/1114 (the 'Markets in Crypto-assets Regulation' or MiCAR) applies. The objective of MiCAR is to establish uniform requirements for crypto assets within the EU, in order to support innovation and fair competition, ensure high levels of protection for consumers and market integrity, and address potential risks to financial stability and monetary policy. The Regulation applies to natural and legal persons engaged in issuing or providing services related to crypto assets in the EU, regardless of their place of establishment or residence. MiCAR excludes from its scope crypto assets that are unique and non-fungible (NFTs), crypto assets qualifying as financial instruments or other regulated products (eg, Electronic Money Directive,[94] the Payment Services Directive,[95] etc) and digital art, collectibles and crypto assets representing unique and non-fungible services or physical assets.

Moreover, although not specifically referring to the metaverse, there is a series of policies and guidance provided by the European Supervisory Authorities in relation to regulated crypto assets.

NFTs and other digital assets that are not currently regulated are subject to the overall EU and national legal frameworks in relation to transactions, ownership, consumer protection and intellectual property rights, while sector-specific provisions that may apply depend on the particular characteristics of the NFT.

In this regard, over the past three years the European Commission and European Parliament have been actively publishing reports and studies on the metaverse and digital assets in the Web 4.0 and virtual environment. While an exhaustive list of the reports and initiatives published exceeds the scope of the present article, one of the most recent policies was published by the European Commission in July 2023, entitled 'An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition'.[96]

The Communication encourages the creation of Web 4.0 and virtual worlds that reflect EU values and principles and fundamental rights, where people can be safe, confident and empowered, where people's rights as users, consumers, workers or creators are respected, and where European businesses can develop world-leading applications, scale up and grow. In this regard, the Communication takes into consideration the different stakeholders of virtual worlds and Web 4.0, such as citizens, academia, civil society, businesses and public authorities. In this document, there is a brief reference to the significant role and challenges posed by NFTs and digital assets.

94 Directive 2009/110 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7.
95 Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010 and repealing Directive 2007/64/EC [2015] OJ L337/35.
96 An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the Next Technological Transition COM(2023) 442 final (European Commission, July 2023).

Q 2. Are there any relevant policies, strategies or regulations applicable to digital transactions in the metaverse in your jurisdiction?

There are various relevant policies, strategies and regulations applicable to digital transactions and ownership in the metaverse in the EU, covering aspects such as consumer protection, contract law, intellectual property, taxation and anti-money laundering. Some of the main instruments are:

- the Consumer Rights Directive and the Unfair Commercial Practices Directive, which provide rules on information, transparency and fairness for online transactions between traders and consumers, as well as remedies and enforcement mechanisms;
- the Digital Content Directive[97] and the Sale of Goods Directive,[98] which harmonise the rules on conformity, liability and remedies for contracts for the supply of digital content or digital services, or for the sale of goods with digital elements, respectively;
- the Intellectual Property Rights Enforcement Directive[99] and the Copyright Directive,[100] which establish a framework for the enforcement of intellectual property rights in the digital environment, as well as specific rules for the use of protected works and other subject matter by online platforms and users;
- the VAT Directive[101] and the E-Commerce VAT Package, which lay down the rules and obligations for the taxation of digital services and goods supplied online within or outside the EU;
- the Anti-Money Laundering Directive and the Markets in Crypto-Assets Regulation, which set out the requirements and standards for the prevention, detection and reporting of money laundering and terrorist financing risks associated with virtual currencies and crypto-assets;
- the Representative Actions Directive,[102] which enables qualified entities to bring actions for the protection of the collective interests of consumers in cases of infringements of EU law by traders;
- the Unfair Terms in Consumer Contracts Directive,[103] which applies to contractual terms which have not been individually negotiated and which are unfair if they cause a significant imbalance in the parties' rights and obligations, to the detriment of the consumer;
- the Digital Services Act, which introduces new rules and responsibilities for intermediary services that offer access to or host user-generated content or facilitate online interactions, such as social networks, online marketplaces or cloud services; and
- the Promoting Fairness and Transparency for Business Users of Online Intermediation Services Regulation,[104] which ensures that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities.

In addition, the creation and sale of NFTs is usually regulated contractually via the specific terms and conditions of the platform. These terms vary depending on the characteristics of the product or service and of the underlying asset that the NFT represents. Nonetheless, since NFTs are a representation of a digital or physical asset, national civil codes will also apply to their sale. Please refer to question 3 below for more details.

In terms of case law, there are no decisions by the European Court of Justice (ECJ) in this regard. However, national courts may have to deal with disputes arising from digital transactions and ownership in the metaverse, depending on the applicable law and jurisdiction clauses.

97 Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.
98 Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.
99 Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L195/16.
100 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29 [2019] OJ L130/92.
101 Directive 2006/112/EC on the common system of value added tax [2006] OJ L347/1.
102 Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L49/1.
103 Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.
104 Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.

3. How is property defined in the metaverse? Are there any relevant policies, strategies or regulations applicable to ownership of digital assets in the metaverse in your jurisdiction?

The question of how property is defined in the metaverse is not straightforward in the EU region as there are different types and forms of digital assets that may be considered to be property, such as virtual land, items, currencies or identities.

There are no specific EU policies, strategies or regulations that apply to ownership of digital assets in the metaverse, and the legal status and ownership rights of these assets may vary depending on the terms and conditions of the platforms, the contractual arrangements between the parties and the applicable national laws. Property law is fragmented in the EU, and the rules on ownership/entitlement will depend on national law provisions, the nature of the asset, whether it is a representation of an underlying asset or a natively digital asset and whether it is subject to mandatory registration. For example, a digital asset could qualify as digital content or could be equated to the nature of the asset that it is representing, such as real estate, movable property or intellectual property.

In any case, most Member States, irrespective of their differences, recognise that every item of property should have the following characteristics: (1) uniqueness; (2) allocation to a specific owner; and (3) exclusion of the ownership by another person. In addition to these minimum characteristics, different approaches are followed among EU Member States and therefore, the nature of digital property may be subject to different interpretations and decisions by national courts.

Moreover, in relation to ownership, the EU intellectual property framework is at the epicentre in this regard. These frameworks provide some protection and rights for the creators of digital content, as well as places some obligations and restrictions on users and intermediary service providers using these digital works. However, these frameworks may not fully address the specificities and challenges posed by the metaverse, such as interoperability, portability and traceability of digital assets, the allocation of liability and responsibility and the enforcement of rights and remedies.

There is no case law or any decisions by a regulator regarding ownership of digital assets in the metaverse in the EU region, as this is a novel and emerging area.

Moreover, there is some case law and decisions by regulators regarding infringements of the general EU intellectual property frameworks in the EU region that, although not specifically related to the metaverse, may be of interest. For example, the CJEU has ruled on several cases involving the interpretation and application of the Database Directive[105] and the Trade Secrets Directive.[106] Particularly relevant is *Bezpecnostni Softwarova Asociace - Svaz Softwarove Ochrany v Ministerstvo Kultury*[107] where it was determined by the ECJ that while graphic user interfaces (GUIs) may not qualify as computer programs under the Software Directive[108] and therefore are not protected by it, they can still be regarded as artistic works. As such, they are eligible for copyright protection, provided that the GUI is an original creation of the author.

This case may provide some guidance and precedent for future cases involving digital assets in the metaverse, but it may also reveal some gaps and uncertainties in the current legal framework.

4. How are property transfers regulated in your jurisdiction?

In the EU, property transfers are governed by a combination of EU and national laws, depending on the type and nature of the property involved. For tangible property, such as goods or real estate, the Rome I Regulation[109] and the Brussels

105 Directive 96/9/EC on the legal protection of databases [1996] OJ L77/20.
106 Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1.
107 *Bezpecnostni Softwarova Asociace - Svaz Softwarove Ochrany v Ministerstvo Kultury* (C-393/09) EU:C:2010:816; [2011] ECDR 3.
108 Directive 91/250/EEC on the legal protection of computer programs [1991] OJ L122/42, now repealed by Directive 2009/24/EC on the legal protection of computer programs [2009] OJ L111/16.
109 Regulation (EC) 593/2008 on the law applicable to contractual obligations [2008] OJ L177/6.

I Regulation[110] determine the applicable law and jurisdiction, respectively. These regulations offer general rules and exceptions in regard to cross-border contracts and disputes within the EU.

For intangible property, such as intellectual property or crypto assets, the applicable law and jurisdiction may vary depending on the specific rights and obligations involved, as well as the existence of harmonised or common rules at the EU level and, of course, the legal status and treatment of crypto assets (eg, financial instruments, electronic money, NFTs, etc).

There is no case law or any decisions by a regulator regarding property transfers of digital assets in the metaverse in the EU region.

Q 5. How are currencies, including cryptocurrencies, used in the metaverse regulated in your jurisdiction? Who are the main stakeholders and what are their obligations?

The regulation of currencies, including cryptocurrencies, used in the metaverse is not uniform or subject to a specific piece of regulation in the EU region, but it may be subject to some general EU legal frameworks that apply to different aspects of these instruments, such as their issuance, transfer, exchange, storage, service provision, anti-money laundering, consumer protection and market integrity. The applicable rules will depend on the nature, function and characteristics of these instruments, such as the Electronic Money Directive, the Payment Services Directive, the Markets in Crypto-Assets Regulation, the Anti-Money Laundering Directive, the MiCAR and the Regulation for a pilot regime for market infrastructures based on distributed ledger technology (DLT Pilot regime).

The main stakeholders involved in the use of these currencies are the users, the platforms and the service providers. Their obligations may vary depending on the type of currency, the type of service and the type of activity, but they may include licensing, registration, reporting, disclosure, due diligence, consumer protection and prudential requirements.

Depending on the specific circumstances and context, non-compliance with the applicable regulations and obligations related to the currencies used in the metaverse may result in various sanctions, such as fines, penalties, injunctions, bans, suspensions, revocations, confiscations, forfeitures, seizures, arrests, prosecutions, convictions, imprisonment or other civil, criminal or administrative actions or remedies. The sanctions may be imposed by the competent authorities or regulators, or by the courts or tribunals, depending on the nature and severity of the breach and the jurisdiction and legal system involved.

Q 6. How are transactions and the ownership of assets in the metaverse taxed in your jurisdiction? What sanctions (civil, criminal, administrative) may apply for non-compliance with these obligations?

The taxation of transactions and ownership of assets in the metaverse, such as cryptocurrencies and NFTs, is not harmonised in the EU and depends on the national laws and practices of each Member State.

The taxation of transactions and ownership of assets in the metaverse, a virtual environment where users can interact, create and trade digital content, may depend on the nature, value and location of the assets, as well as the legal status and residence of the parties involved.

Transactions involving the exchange of fiat currency, cryptocurrency or other digital tokens for metaverse assets may be subject to income tax, capital gains tax, value-added tax (VAT) or other applicable taxes, depending on the circumstances and the tax treatment of the underlying assets and tokens.

The use of cryptocurrency or other digital tokens as a means of payment may also trigger tax implications, such as income tax or capital gains tax on the exchange rate gains or losses, or VAT on the supply or acquisition of the tokens.

110 Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.

In this regard, it should be noted that according to the ECJ's decision in *Skatteverket v Hedqvist,*[111] transactions involving cryptocurrencies, such as exchanging them for traditional currencies or mining them, are exempt from VAT, as they are considered to be services supplied for consideration that are closely linked to the payment system. However, the VAT treatment of NFTs may vary depending on the nature and characteristics of the underlying asset and the contractual arrangements between the parties.

The income tax and capital gains tax implications of transactions and ownership of assets in the metaverse are also subject to the national rules and definitions applied in each Member State. Some Member States may treat cryptocurrencies and NFTs as intangible assets, others as financial instruments, and others as commodities or property. Depending on the classification, different tax rates, deductions, exemptions and reporting obligations may apply.

Furthermore, some Member States may have specific anti-money laundering and anti-tax evasion rules that require the identification and verification of the parties involved in transactions with cryptocurrencies and NFTs, as well as the disclosure and exchange of information with the tax authorities.

Non-compliance with the applicable tax obligations may result in various sanctions, depending on the type and severity of the infringement and the national legal framework applicable-. Sanctions may include fines, penalties, interest, confiscation, seizure, freezing, injunctions, suspension, revocation or cancellation of licences, permits, or registrations, as well as criminal prosecution and imprisonment in some cases. Therefore, it is advisable to consult a tax professional before engaging in transactions or owning assets in the metaverse, as the tax consequences may be complex and uncertain.

Q 7. Are there any upcoming policies, strategies or regulations that will impact digital transactions in your jurisdiction?

Over the past three years, both the European Commission and European Parliament have been actively releasing reports and studies concerning the metaverse and digital assets within the context of Web 4.0 and virtual environments. While providing an exhaustive list of these reports and initiatives is beyond the scope of this discussion, one of the latest policies published by the European Commission, entitled 'An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the Next Technological Transition', was issued in July 2023.[112] Additionally, in January 2024, the European Commission initiated a public consultation on competition within virtual worlds.

These two initiatives illustrate the European Commission's interest in potentially regulating virtual worlds in the medium term, which could significantly influence how transactions and digital assets are treated across the EU.

Aside from anticipating the outcomes of the public consultation on competition in virtual worlds and potential initiatives stemming from the European Commission's communications, the application of the following regulations may be particularly pertinent for digital transactions and asset ownership within the metaverse:

- the implementation of the DSA and DMA will have a significant impact on digital transactions in the metaverse, in terms of how platforms are held accountable for illegal or harmful content, how they manage data and interoperability, and how they prevent anti-competitive practices and ensure market access; and
- the implementation of the three pillars of the EU's Data Strategy – the Data Governance Act, Data Act and Common European Data Spaces initiatives – could potentially impact digital transactions in the metaverse in terms of how data is shared, accessed and used by different actors, such as data intermediaries, data altruism organisations or public sector bodies. See the chapter on data for the EU approach on data in the metaverse.

Considering the convergence of metaverse and AI technologies, the recently approved Artificial Intelligence Act (AIA) is of particular importance. The AIA could potentially affect digital transactions in the metaverse in terms of how AI systems are classified, assessed and monitored for compliance with ethical and legal standards, as well as how users are informed and protected from potential harms or biases. See the chapter on AI and the metaverse for more information on the EU approach to AI in the metaverse.

111 *Skatteverket v Hedqvist* (C-264/14) EU:C:2015:718; [2016] STC 372.
112 An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the Next Technological Transition (COM(2023) 442 final) (European Commission, July 2023).

8. Are there any upcoming policies, strategies or regulations that will impact ownership of assets in the metaverse in your jurisdiction?

See the response to the question above.

Liability and insurance

Eric Wagner *Gleiss Lutz, Stuttgart*
Marc Ruttloff *Gleiss Lutz, Stuttgart*

Q 1. Are there any relevant policies, strategies or regulations applicable to liability in the metaverse in your jurisdiction?

At present, liability issues still have to be clarified under general civil law, in particular the law of obligations, tort law and product liability law, as there are no AI-specific liability regulations yet. However, in order to make the most of the economic and social benefits of AI and promote digital economic change, the European Commission submitted a proposal for a directive on 28 September 2022 to adapt the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive),[113] while the law of obligations remains untouched. In connection with the AI Act and the AI Liability Directive, a directive on liability for defective products was also proposed, which is intended to adapt product liability law.[114] The AI Liability Directive does not explicitly mention the metaverse. However, it has been expressly confirmed in the past that the AI Act also applies to the metaverse and that no further regulations need to be issued. It is therefore obvious that the AI Liability Directive must also apply to non-contractual liability issues in the metaverse. However, on 17 January 2024, the European Parliament dealt with the European Commission's strategy on the Web 4.0 initiative and virtual worlds[115] and called on the European Commission to review the effectiveness of existing legislation on a permanent basis and to adopt new legislation if necessary.[116] That is why the metaverse may soon have its own liability rules if the AI Liability Directive is unable to achieve its desired effects in the metaverse.

Q 2. Are there any relevant policies, strategies or regulations applicable to insurance for damages caused in the metaverse in your jurisdiction?

For the third year in a row, cyber incidents are the biggest business risk for companies, even ahead of business interruptions.[117] They are estimated to cost companies more than a trillion dollars a year and therefore represent an area that is in urgent need of insurance against such risks.[118] In order to prevent such damage, it is possible to take out so-called cyber risk insurance policies, for which the German Insurance Association (GDV) has issued model agreements that include general insurance conditions.[119] Such insurance options also exist in some cases for consumers who, for example, have made costly investments in NFTs in the metaverse and are therefore also in need of protection.[120] In some cases, however, cyber risks are also covered by household liability or legal expenses insurance.[121] In this context, VR glasses,

113 Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (Directive on AI Liability), COM (2022) 496 final, 2022/0303(COD), 29 September 2022.
114 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM (2022) 495 final, 2022/0302(COD), 29 September 2022.
115 *Auf dem Weg zum nächsten technologischen Wandel: Kommission stellt EU-Initiative für das Web 4.0 und virtuelle Welten (Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds** *Publisher's translation) (European Commission, 11 July 2023), https://ec.europa.eu/commission/presscorner/detail/de/IP_23_3718, accessed 7 March 2024.
116 *Policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues* (European Parliament, 17 January 2024), www.europarl.europa.eu/doceo/document/TA-9-2024-0029_EN.html, accessed 7 March 2024.
117 Simon Heetkamp in Hans Steege and Kuuya Chibanguza, Metaverse Rechtshandbuch (Nomos, 2023), § 26 p 435; Allianz Risk Barometer 2024, https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf, accessed 7 March 2024.
118 *Ibid*.
119 GDV, 'Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung' ('General insurance condition of cyber risk insurance'* *Publisher's translation) (AVB Cyber), Musterbedingungen des GDV (Stand: February 2024), www.gdv.de/resource/blob/6100/c039bc8e50b81e0da68d3c865b0ea65d/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung-avb-cyber--data.pdf, accessed 8 March 2024.
120 Heetkamp in Steege and Chibanguza, Metaverse Rechtshandbuch (2023), s 26 p 435 f.
121 *Ibid*.

which are important for the metaverse, are currently causing trouble, as they are the cause of an increasing number of accidents and claims.[122] The British insurer Aviva reported a 31 per cent increase in VR insurance claims in 2021 compared to 2020.[123] However, it is questionable whether the existing insurance framework is sufficient for the specifics of the metaverse. It is therefore worth considering whether separate, tailor-made insurance products should be developed for the metaverse.[124]

Q 3. What are the civil liability/tort liability rules applicable to the metaverse in your jurisdiction? Who are the responsible stakeholders in the case of damages?

In the absence of special regulations, the principles of general civil law must be applied, according to which the person who has culpably violated an obligation or a legal interest is liable. However, the planned AI Liability Directive now creates the basis for special non-contractual, fault-based liability, which will also be applicable in relation to the metaverse. The draft directive assumes that providers, as well as operators and users, can be 'defendants' and, therefore, does not impose liability risk on a single actor.

However, it remains to be seen how the directive will be implemented by the Member States, as the latter will be given the option of structuring it as strict liability, which will affect the operators. In the event of damage occurring, the latter would then be liable for the damage regardless of fault.

Q 4. How are liability rules enforced in the metaverse in your jurisdiction? Who are the responsible stakeholders in the case of damages?

There is almost no literature on law enforcement in the metaverse due to a lack of evidence. The decentralised structure of the metaverse poses challenging problems with regard to law enforcement, particularly because the applicable law and the place of jurisdiction are difficult to determine.[125] The desire of metaverse users for anonymity does not simplify the situation either.[126] Platform liability is therefore likely to play a major role.[127] Overall, however, it is not be possible to give a general answer to the question due to the many inconsistencies currently at play.

Q 5. What are the roles of intermediaries and gatekeepers when it comes to enforcement of rights and liability on the metaverse?

Due to the general uncertainties and lack of information, this question cannot be answered in a generalised and brief manner.

122 'Zu viele zerstörte Fernseher: Aviva warnt vor Virtual-Reality-Brillen' ('Too many destroyed TVs: Aviva warns against virtual reality glasses'* *Publisher's translation) (Versicherungswirtschaft-heute, 17 February 2022), https://versicherungswirtschaft-heute.de/politik-und-regulierung/2022-02-17/zu-viele-zerstoerte-fernseher-aviva-warnt-vor-virtual-reality-brillen/, accessed 8 March 2024.

123 'Zu viele zerstörte Fernseher: Aviva warnt vor Virtual-Reality-Brillen' (Versicherungswirtschaft-heute, 17 February 2022); T. Gangcuangxo, 'Virtual reality and insurance claims – Aviva reveals link' (*Insurance Business UK*, 14 February 2022), www.insurancebusinessmag.com/uk/news/technology/virtual-reality-and-insurance-claims--aviva-reveals-link-325330.aspx, accessed 8 March 2024.

124 See n 123 above, 436.

125 Fabian Reinholz, Metaverse und Recht: Das Recht des Metaverse – ein Überblick (GRUR-Prax, 2023, 478), p 481.

126 David Quinke, Florian Wagner and Björn Ebert in Wagner, Holm-Hadulla and Ruttloff, *Metaverse und Recht* (2023), s 1 Rn. 16.

127 See n 128 above.

Q 6. What are the relevant insurance topics regarding the metaverse in your jurisdiction?

As previously mentioned, VR glasses, which are important for the technical implementation of the metaverse, are currently causing trouble as they are the cause of more and more accidents and claims.[128] The British insurer Aviva reported a 31 per cent increase in VR insurance claims in 2021 compared to 2020.[129] According to Aviva, the average claim made in such cases last year was around £650 (around €780).[130] As an example (in an extremely entertaining way), the countless VR fail video compilations on YouTube impressively illustrates the most curious claims. In the future, hacker attacks in the metaverse will be an insurance-relevant topic.[131] Hackers could attempt to gain unauthorised access to user's biometric data through VR glasses, manipulate users by changing the environment or deceive them about the identity of avatars with malicious intentions.[132] As a result, users could be tricked into disclosing personal data, which could be used by hackers, for example, to cause damage.[133] Hackers could also seize the victim's digital identity.[134]

Q 7. Are there any relevant policies, strategies or regulations applicable to criminal liability in the metaverse in your jurisdiction?

At present, there is no specific AI or metaverse criminal law, meaning that any criminal liability must be assessed according to general criminal law. The applicability of German criminal law is based, in particular, on the principles of 'internet-based offences' developed through case law and the literature.[135] Three different directions of action relevant under criminal law are conceivable: actions of the avatar in the metaverse, actions of natural persons in setting up/the operation of virtual spaces and actions of natural persons outside the metaverse with reference to the metaverse.[136] All of these types of actions can be comprehensively covered and regulated by German criminal law.[137] Consequently, criminal liability is determined according to the general rules of attribution, so that in the case of avatar actions, for example, the user's control commands could constitute a criminal offence. Nevertheless, as time goes on and technology advances, situations will arise that will not be captured by the legal framework, such as the actions of an avatar, combined with the effect of the action in the virtual world, which still in no way can be compared with corresponding events in the real world.[138] While the EU is currently focusing, in particular, on the use of AI in criminal (procedural) law,[139] no new AI- or metaverse-specific criminal norms are currently being developed.

Q 8. Are there any upcoming policies, strategies or regulations impacting liability (civil/tort/criminal) in the metaverse in your jurisdiction?

In order to make the most of the economic and social benefits of AI and promote digital economic change, the European Commission submitted a proposal for a directive on 28 September 2022 to adapt the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive),[140] while the law of obligations remains untouched. In connection with the AI Act and the AI Liability Directive, a directive on liability for defective products was also proposed, which

128 'Zu viele zerstörte Fernseher: Aviva warnt vor Virtual-Reality-Brillen' (Versicherungswirtschaft-heute, 17 February 2022).
129 'Zu viele zerstörte Fernseher: Aviva warnt vor Virtual-Reality-Brillen' (Versicherungswirtschaft-heute, 17 February 2022); Gangcuangxo, 'Virtual reality and insurance claims – Aviva reveals link' (*Insurance Business UK*, 14 February 2022).
130 Armin Nadjafkhani, 'VR-Brillen lassen Schadensmeldungen steigen' (*Future Zone*, 14 February 2022), https://futurezone.at/digital-life/virtual-reality-sachschaeden-versicherung/401905351, accessed 8 March 2024.
131 See n 123 above, 436.
132 See n 123 above, 436; Kaulartz, Schmid and Müller-Eising, *Das Metaverse – eine rechtliche Einführung* (2022, 521), p 525 Rn. 26.
133 See n 123 above, 437.
134 *Ibid*.
135 Arne Klaas and Kathrin Klose in Steege and Chibanguza, *Metaverse Rechtshandbuch* (2023), § 32 p 534 ff., 559.
136 *Ibid*.
137 *Ibid*.
138 *Ibid*.
139 *Künstliche Intelligenz im Strafrecht (Artificial Intelligence in criminal law** *Publisher's translation) (European Parliament), www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS_ATA(2021)698039_DE.pdf, accessed 8 March 2024.
140 Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (Directive on AI liability), COM (2022) 496 final, 2022/0303(COD), 29 September 2022.

is intended to adapt product liability law.[141] It will be interesting to see how each national legislator implements the legislation.

Q 9. Are there any upcoming policies, strategies or regulations related to insurance in the metaverse in your jurisdiction?

No, the development of such policies, strategies or regulations is not apparent at the time of writing.

141 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM (2022) 495 final, 2022/0302(COD), 29 September 2022.

Jurisdiction and governance

Eric Wagner *Gleiss Lutz, Stuttgart*
Marc Ruttloff *Gleiss Lutz, Stuttgart*

Q 1. Are there any upcoming policies, strategies or regulations setting out rules on how to identify the governing law in the metaverse?

Due to the decentralised and interoperable structure of the metaverse, platform operators allow a broad mass of users from all over the world to participate and this is typically governed by a platform usage agreement.[142] Since the latter typically has a cross-border dimension within the meaning of Article 3 of the Einführungsgesetz zum Bürgerlichen Gesetzbuche (EGBGB), the applicable law must be determined in each individual case in accordance with the principles of private international law.[143] However, a metaverse-specific, standardising regulation of this kind does not yet exist and is not in sight.

Q 2. Are there any upcoming policies, strategies or regulations setting out rules on how to identify the jurisdiction in the metaverse? Is there any case law or are there any decisions by a regulator regarding determining jurisdiction in the metaverse in your jurisdiction?

As long as the general terms and conditions do not stipulate a jurisdiction or arbitration agreement and the platform does not provide for an internal dispute resolution mechanism, the general rules of jurisdiction apply, which, in addition to the German Code of Civil Procedure (ZPO), also includes the rules of international jurisdiction of the courts, for example those of the *EuGVVO,* which must be observed as a matter of priority.[144] According to the principle of dual jurisdiction of the local jurisdiction rules,[145] the court with local jurisdiction under German law also has international jurisdiction.[146] Problems in determining jurisdiction can, however, be caused by users' wishes for anonymity, as the general place of jurisdiction cannot be determined in this way, which is why special places of jurisdiction in relation to the metaverse may become more relevant.[147] As with the question of applicable law, however, there are no rules or strategies on the question of the applicable jurisdiction and none are currently being planned.

Q 3. What are the competent regulators and government bodies tasked with ensuring compliance with the applicable laws in the metaverse in your jurisdiction?

The metaverse is mainly regulated by the AI Act. The AI Act is based on a broadly diversified system of authorities that provides for numerous bodies with different responsibilities at both national and European level, which are obliged to cooperate with each other.

142 Christoph Wendelstein in Steege and Chibanguza, Metaverse Rechtshandbuch (2023), s 9 p 183.
143 Moritz Hollm-Hadulla, Eric Wagner and Martin Viciano Gofferje, 'Digital Economy: Virtuelle Realität – Metaverse-Plattformen und ihre rechtlichen Fragen' ('Digital Economy: Virtual reality – metaverse platforms and the legal issues'* *Publisher's translation) (Gleiss Lutz, 19 July 2022), www.gleisslutz.com/de/aktuelles/know-how/virtuelle-realitaet-metaverse-plattformen-und-ihre-rechtlichen-fragen, accessed 8 March 2024.
144 David Quinke, Florian Wagner and Björn Ebert in Wagner, Holm-Hadulla and Ruttloff, *Metaverse und Recht* (2023), s 1 Rn. 4.
145 BGH, Urt v. 18. 1. 2011 – X ZR 71/10 (OLG Frankfurt a. M.), BGH NJW 2011, 2056, Rn. 18; BGH, Urteil vom 18-04-1985 – VII ZR 359/83 (Karlsruhe/Freiburg), BGH NJW 1985, 2090.
146 See n 147 above.
147 *Ibid*.

At European level, there is the AI Office, the European Committee on Artificial Intelligence, the Advisory Forum and the Scientific Panel of Independent Experts. The AI Office[148] acts as the central body and right hand of the European Commission and carries out all necessary measures to ensure the effective enforcement of the Ai Act. The European Artificial Intelligence Committee[149] supports the European Commission and the AI Office and contributes, for example, to the coordination and support of national authorities. The Consultative Forum[150] provides technical expertise in consultation with the Committee and the Commission. The Scientific Panel of Independent Experts[151] advises and supports the AI Office in relation to general-purpose AI (GPAI) models through risk warnings, tool and method development for capability assessment, classification advice, benchmark setting and template development.

At national level, there are the notifying bodies, the notified bodies and the market surveillance authorities. Notified bodies are conformity assessment bodies that have been licensed and commissioned, ie, notified, by notifying bodies.[152] Most important, however, are the national market surveillance authorities, whose tasks and competences are reflected throughout the entire regulatory framework. The market surveillance authorities are mainly responsible for market surveillance and control and, thus, for enforcing the AI Act, for which they have been given numerous powers. However, it is not yet clear which exact authority in Germany will assume the role of market surveillance authority.

Q 4. Are there any available dispute resolution mechanisms in your jurisdiction?

In addition to the courts[153] and arbitration tribunals,[154] there may also be internal dispute resolution mechanisms within the specific platform.[155] In addition, Article 68a onwards of the AI Act provides for special legal remedies, such as a right of appeal to the competent market surveillance authority in Article 68a(1), regardless of affection. However, there are no regulations that provide for specific dispute resolution mechanisms for the metaverse.

Q 5. How is arbitration implemented in the metaverse in your jurisdiction?

In contrast to many other areas of law, international arbitration has been dedicated to the metaverse for some time, with the 'first ever Virtual Reality Arbitration Conference' taking place in the metaverse on 30 March 2022.[156]

Metaverse disputes will represent a considerable effort for national and international arbitration tribunals, as several platform operators have already included arbitration agreements in their terms of use.[157] For the metaverse, 'online dispute resolution', which became popular in the wake of the Covid-19 pandemic through online arbitration proceedings, could become highly relevant, even if it is not clear how the decisions made, possibly in the form of digital arbitration awards, can be recognised and enforced in the real world.[158] Oral hearings by video conference and the use of electronic documents and evidence also offer excellent opportunities.[159] In addition, arbitration courts are already giving in more to requests for anonymity, so that (limited) identity-obscuring hearings in the metaverse via VR glasses also appear possible in principle.[160]

Even if the German Code of Civil Procedure (ZPO) (still) nips the idea in the bud, efforts are even being made in other countries to make the metaverse an 'anational' place of arbitration in order to avoid state restrictions.[161]

148 AI Act, Art 55b.
149 *Ibid* , Art 56 onwards.
150 *Ibid* , Art 58a.
151 *Ibid* , Art 58b.
152 *Ibid* , Arts 43 and 44.
153 See n 147 above, Rn 1 ff.
154 *Ibid* Rn 21 ff.
155 *Ibid* Rn 4.
156 'Paris Arbitration Week Recap: Metaverse-Related Sessions' (Kluwer Arbitration Blog, 24 April 2022), https://arbitrationblog.kluwerarbitration.com/2022/04/24/paris-arbitration-week-recap-metaverse-related-sessions/, accessed 8 March 2024.
157 See n 147 above, Rn 26.
158 *Ibid*, Rn 27, 28, 32.
159 *Ibid*, Rn 29.
160 *Ibid*, Rn 30.
161 *Ibid,* Rn 31.

As a result, arbitration presents a colourful bouquet of possibilities, but also challenges, in regard to the metaverse, the developments of which will be followed with interest in the future.

Q 6. Are there any upcoming policies, strategies or regulations regarding determining governing law and jurisdiction in the metaverse in your jurisdiction?

As mentioned in the responses above, there are no policies, strategies or regulations that define the applicable law and jurisdiction in the metaverse. In terms of jurisdiction, the metaverse is still a blank slate.