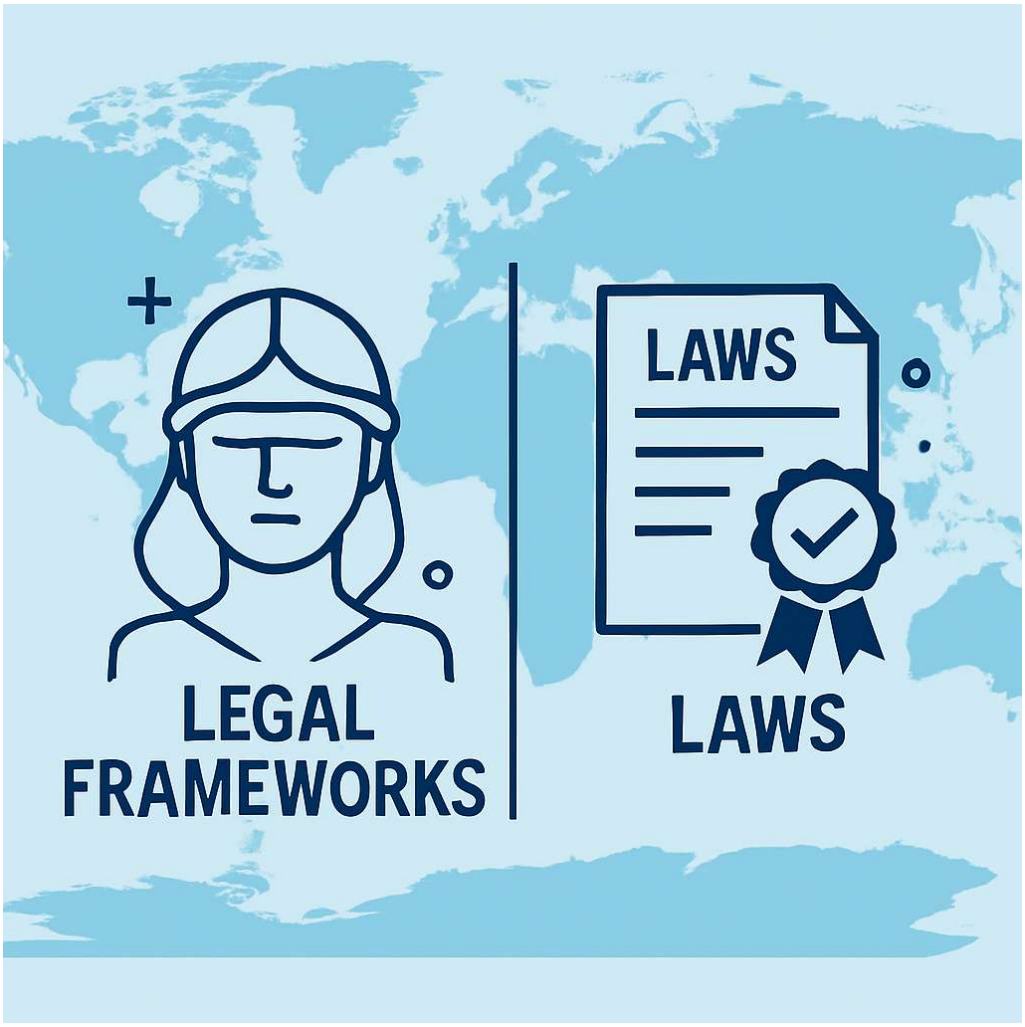
Analysis of the Impacts of European Union Legal Frameworks and Laws on Virtual Worlds



June 2025

Report Prepared and Published Jointly by

VIRTUAL DIMENSION CENTER

Virtual Dimension Center (VDC) and PEREY Research & Consulting

DOI: 10.6084/m9.figshare.29400107

NOTE: This report is not an ETSI document and is not a deliverable of the STF 686 ViWISSO project.

Acknowledgement

The authors wish to thank Jacqueline Watts, principal of A City Law Firm Ltd for her review and feedback of a draft of the present report.

About the authors

Christoph Runde is a senior standardization expert. With more than 25 years of VR industry experience, he is a pioneer in the field of professional systems and applications of virtual reality and augmented reality. After starting his career at Porsche, he joined the Fraunhofer Institute for Manufacturing Engineering and Automation (IPA) in 1999, where he led the institute's activities in VR/AR. Beginning in 2007 he developed the Virtual Dimension Center (VDC) into one of the biggest and most successful cluster initiatives for VR/AR in Europe.

In parallel to his position as director of VDC, Christoph Runde is professor for Virtual Reality at the Heilbronn University. In the European Association for eXtended Reality (EuroXR) he works as Vice President Industry and End Users. Christoph Runde is the author of the largest database on XR and MV related norms, standards, specifications, guidelines, recommendations, working groups and standard development organizations. He is also the co-chair of the Metaverse Standards Forum's Standards Register WG.

The Virtual Dimension Center (VDC) is Germany's leading competence network for Virtual Engineering. Technology and service providers, users, research institutions and multipliers work together in the VDC network along the entire value chain of Virtual Engineering- namely in 3D simulation, 3D visualization, product lifecycle management (PLM), and Virtual Reality (VR). The VDC maintains a liaison with ISO-IEC JTC1/SC24 Computer graphics, image processing and environmental data representation, and memberships with the Alliance for OpenUSD, App Defense Alliance, Simulation Interoperability Standards Organization (SISO), IEEE Standards, and the Khronos Group.

Christine Perey is a Spime Wrangler. She leads and joins teams working collaboratively to advance business prospects in new technology markets where space and time intersect. Bruce Sterling first used the neologism "Spime" in August 2004 at SIGGRAPH that year. He predicted then that at the intersection of space and time, Spimes would arise. Sterling said "true Spimes create spime wranglers. Wranglers are the class of people willing to hassle with Spimes. And it is a hassle. An enormous hassle. But it's a fruitful hassle. It is the work of progress. Handled correctly, it can undo the harm of the past and enhance what is to come."

PEREY Research and Consulting provides industry-specific knowledge and services packaged the way businesses in fast-moving markets need them—concise, concrete and actionable. Companies leverage the value they receive from working with us in business plans and formulating a variety of mission-critical decisions. We offer agencies of all types, investors, service providers and technology vendors who want to expand their mobile augmented reality communications and community opportunities the tools and the professional partnerships that they need.

Contents

1 Introduction

This report provides insights about the relevance and current or potential future impacts of 34 European and national legal frameworks or laws currently being enforced across the European Union on virtual world technology development and adoption.

Table 1: Legal frameworks and laws relevant for virtual worlds

Advertising	Design law	Legal protection and jurisdiction
Banking and capital market law	Digital identities	Media law
Commercial law	Fair trade	Medical and medical device law
Company law	Financial supervisory law	Patent law
Competition and antitrust law	Financial transactions	Police law and state control
Consumer protection	Gambling law	Private international law
Contract law	Gaming and eSports	Right of personality
Copyright law	Insurance law	Supply chain law
Criminal liability	Intellectual property	Tax law
Cyber security	Labour law	Tenancy and residential property
Data protection	Lawyers professional law	Trademarks
		Use of standards: legal implications

The topics in this report, listed in the table 1 above, are organized alphabetically. In each section there is a short explanation of the topic followed by how the topic applies to virtual worlds.

The sections also describe if and how their definition could need to be refined to cover virtual worlds and when or how they could have impacts on the enforcement of the laws or frameworks in immersive experiences.

2 Advertising

Advertising law in virtual worlds is shaped by national systems as well as European and international frameworks. Central at the European level is the Digital Services Act (DSA), which requires transparent practices by platforms and advertisers. The EU Directive on Unfair Commercial Practices also applies, especially concerning the labelling of advertising. Given the global reach of virtual world technologies and platforms, advertisers must account for international regulatory differences and local legal expectations.

The legal foundations rely on three key principles: transparency, fairness, and the avoidance of misleading content. Advertising must be clearly recognizable to avoid covert messaging. Statements must be accurate and include all essential details for user decisions. Legal protection also extends to preserving fair market conditions and preventing monopolistic behaviour. In global digital spaces, respecting cultural norms becomes a significant factor in ensuring ethical and legal advertising.

In the evolving environment of virtual worlds, several legal uncertainties arise. Advertising in immersive formats and experiences challenges traditional labelling standards. Influencer marketing through avatars raises the question of disclosure rules and liability. Furthermore, data-driven advertising, often based on behavioural profiling, must comply with privacy rules such as those established in the GDPR, particularly regarding user consent and transparency.

The main legal risks include insufficient or deceptive labelling of advertisements, misleading claims, and manipulative user interfaces, known as dark patterns. Global advertising campaigns may also run into conflicts when content legal in one country is restricted in another. Unauthorized personalized advertising poses a significant data protection risk and may lead to regulatory sanctions.

Best practices involve the visible marking of advertising, clear sponsorship disclosures, and full compliance with the DSA and GDPR. Platforms should actively moderate advertising content. In contrast, hiding promotional intent, omitting critical information, or using manipulative design and unlawfully collected data are considered worst practices and violate established European legal standards.

3 Banking and capital market law

Banking and capital market law in virtual worlds is shaped by European and international regulations, particularly the Markets in Crypto-Assets Regulation (MiCAR) and the Markets in Financial Instruments Directive (MiFID II). These frameworks govern financial services, crypto-assets, and cross-border transactions. As virtual worlds host decentralized and transnational activity, determining the legal scope of supervision becomes complex. Regulatory authorities play a key role in setting clear rules, especially in licensing and compliance expectations for virtual asset service providers.

The core principles include legal certainty, investor protection, and market integrity. Financial service providers must ensure transparency and provide comprehensible information to users. The principle of proportionality applies, allowing the law to adapt to innovative technologies without overregulation. Technological neutrality ensures that new forms of digital assets, such as NFTs, are treated fairly under existing laws. Supervision by independent regulators is essential to prevent systemic risks and ensure market stability in virtual environments.

Legal uncertainties arise particularly in the classification and regulation of digital assets. Questions concern how cryptocurrencies, NFTs, and other virtual assets are to be legally defined, and which regulatory requirements apply to their issuance, custody, or trading. Cross-border service provision complicates matters further, especially when providers are based outside a particular jurisdiction. It remains open whether existing frameworks like MiCAR fully address these new developments. The boundary between licensed and unlicensed activities is also critical.

Key legal risks include insufficient oversight of asset providers, increasing the potential for fraud, money laundering, or manipulation. The unclear classification of certain digital assets also creates loopholes. Investors face dangers from opaque or high-risk offerings. Technological vulnerabilities, such as smart contract failures or cyberattacks, intensify the risk landscape.

Compliant conduct includes obtaining proper licenses, preparing necessary disclosures, and applying MiCAR rules. Illegal conduct includes offering regulated services without authorization, failing transparency obligations, or compromising investor protection through insecure systems.

4 Commercial law

Commercial law in virtual worlds is governed by general contract and trade principles, supported at the European level by regulations such as the Markets in Crypto-Assets Regulation (MiCAR), the eIDAS Regulation, and the Consumer Rights Directive. These frameworks are applied to digital content and virtual goods, including NFTs and tokens, which require legal classification for lawful trade. Regulatory compliance also extends to tax law and data protection under the GDPR, especially where transactions involve personal data or cross-border activities.

The fundamental principles of commercial law include freedom of contract, legal certainty, and transparency. In virtual worlds, these are complemented by distance selling rules, which grant consumers specific protections such as the right of withdrawal. Transparency is especially relevant when dealing with the characteristics and limitations of digital goods. Proportionality ensures a balanced approach between innovation and legal safeguards, while technological neutrality allows for the seamless integration of smart contracts and NFTs within existing legal structures.

Legal challenges include defining whether the transaction of virtual goods constitutes a sale transferring ownership or a license granting usage rights. The scope of warranty and withdrawal rights for purely digital products remains unclear. There is also a legal gap in how to treat hybrid transactions involving both physical and digital components. Further complexity arises when tokens might fall under financial market regulation, demanding full compliance with MiCAR and other relevant rules.

Risks include unclear categorization of NFTs, lack of transparency in digital product descriptions, and weak protection of usage rights, particularly when platforms change terms or remove access. Legal conflicts may also result from jurisdictional ambiguities. Insecure technological implementations, such as faulty smart contracts, increase liability.

Lawful practices involve transparent terms, full consumer rights, and compliant use of smart contracts. Illegal actions include failing to disclose product characteristics, bypassing consumer protections, or violating MiCA through unauthorized token issuance.

5 Company law

Company law in virtual worlds is grounded in existing national and international corporate frameworks, though new challenges emerge with decentralized autonomous organizations (DAOs). DAOs operate without a fixed administrative centre or central management and are often structured around smart contracts and collective decision-making. Their legal classification varies depending on structure and jurisdiction, and in some systems, they may be equated with traditional partnerships, leading to personal liability for members. The absence of formal registration and central authority complicates legal attribution and enforcement.

Core principles include organizational autonomy, decentralized governance via smart contracts, and the role of token-based voting. Legal relationships are defined programmatically, which challenges conventional legal standards regarding contracts, liability, and dispute resolution. The territoriality principle and conflicts in applicable law pose additional issues, particularly in global contexts where jurisdictions differ in recognizing and regulating virtual legal entities.

Key legal questions include whether DAOs can be formally registered and under what legal structure, how liability is assigned in cases of misconduct or unauthorized actions, and whether existing company law provisions are suitable for regulating digital organizations. The lack of a clear governance structure also makes it difficult to assign accountability and protect the rights of stakeholders.

Risks involve legal uncertainty over DAO liability, manipulation risks despite claimed decentralization, and the lack of recognized legal safeguards for automated governance through smart contracts. International regulatory fragmentation adds to the unpredictability, especially in cross-border contexts.

Compliant practices include clear communication of DAO rules, formal registration in jurisdictions that legally recognize such entities, and adherence to smart contract procedures for governance. Illegal conduct includes using DAOs without fulfilling legal form requirements, using smart contracts for unlawful activities, or undermining member rights by manipulating voting mechanisms. These actions may lead to regulatory sanctions or civil liability.

6 Competition and antitrust

Competition and antitrust law in virtual worlds is primarily governed by European law, notably Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), which prohibit anticompetitive agreements and abuse of dominant positions. These rules are supported by the Digital Markets Act (DMA), which specifically targets gatekeeper platforms, and by the EU Merger Regulation, which regulates corporate concentration. The legal framework aims to ensure competitive fairness even in rapidly evolving digital markets and virtual ecosystems.

The key principles include safeguarding free market access, preventing monopolistic structures, and encouraging innovation. Companies are prohibited from forming cartels or engaging in conduct that restricts competition. Abuse of market dominance, such as self-preferencing or exclusive access to infrastructure or data, is also unlawful.

Interoperability is a central concern, especially in virtual environments, to avoid the creation of closed systems that lock in users or exclude competitors. Consumer welfare remains a guiding goal of all antitrust interventions.

Legal challenges include defining what constitutes a relevant market in virtual settings, where services often merge social, economic, and technical functions. Regulatory focus is also directed at merger strategies like killer acquisitions, which aim to eliminate future competitors. Ensuring interoperability among platforms is crucial for maintaining open digital markets and reducing barriers to entry for smaller providers.

Legal risks involve the entrenchment of dominant platforms through anticompetitive behaviour, including the obstruction of rivals via exclusive standards or data access control. Discriminatory practices or the limitation of interoperability can distort competition and lead to enforcement actions by regulators.

Legally compliant behaviour includes cooperation in standard-setting that enhances efficiency without restricting competition, respecting DMA obligations, and structuring mergers transparently. Unlawful practices include collusive agreements, discriminatory access restrictions, and the use of technical standards to exclude market newcomers, all of which are subject to significant legal penalties.

7 Consumer protection

Consumer protection law in virtual worlds is governed by European legal frameworks such as the Consumer Rights Directive and the Digital Services Act (DSA), which apply to digital services and virtual transactions. These regulations aim to ensure that consumer rights remain enforceable even in immersive digital environments. As Metaverse platforms qualify as digital services, they are subject to legal standards concerning transparency, contractual clarity, and user protection.

Core principles include the obligation to provide clear, accessible information about contract terms, pricing, and consumer rights such as the right of withdrawal. Providers of digital goods must guarantee functionality and freedom from defects while ensuring that immersive technologies do not interfere with users' ability to make informed decisions. Virtual avatars, real-time environments, and algorithmic personalization must not undermine consumer autonomy or create unfair commercial advantages.

Legal challenges focus on the applicability of existing consumer protection rules to virtual goods and services. It remains essential to clarify whether users can effectively exercise rights like withdrawal in digital-only transactions. Further complexity arises from the use of personalized advertising or interface designs that could mislead or surprise users, potentially infringing on their legal protections. Platform operators must also meet their information obligations, especially when automated systems influence user choices.

Major legal risks include the use of vague or non-transparent contracts, manipulative advertising methods, and failure to uphold warranty claims for faulty digital products. The decentralized nature of many virtual world use cases can also complicate the enforcement of consumer rights, particularly when providers are anonymous or located in other jurisdictions.

Best practices involve providing clear and complete product information in line with European consumer law, ensuring contract transparency, and honouring user rights regarding defects and returns. Illegal practices include deceptive design, obscured terms and conditions, and the limitation of legal entitlements through technical or psychological manipulation. These violations may trigger sanctions and liability.

8 Contract law

Contract law in virtual worlds is governed by existing legal frameworks applicable to service, purchase, rental, and digital content contracts. These rules apply to typical relationships such as platform use agreements and transactions involving virtual goods like NFTs. Many Metaverse platforms operate in decentralized forms, for example via DAOs, making it difficult to identify contractual partners or enforce claims, especially in cross-border contexts.

Fundamental principles include contractual freedom, consumer protection, and the fulfilment of agreed obligations. Unlike traditional sales, contracts in virtual worlds often grant limited usage rights rather than ownership. Therefore,

transparency in contract design and clear specification of rights and obligations are critical. Digital goods are subject to the same legal recognition as physical goods, provided that legal requirements are met.

Remaining legal challenges include determining the proper classification of contracts involving digital assets, defining user rights in case of disruptions like server outages, and clarifying the enforceability of agreements formed in anonymous or decentralized systems. Systems for defining how a contract can be formed in virtual worlds, especially in an immersive space and how can it be brought to the attention of the parties properly, are not defined differently from those systems for physical world agreements. It remains difficult to pursue claims against international operators, particularly when their legal structure is unclear or extraterritorial.

Legal risks arise from the misclassification of contract types, which may lead to conflicts over usage rights and service obligations. Ambiguity in contract terms can result in legal uncertainty, especially when access to digital goods is revoked or limited without justification. Furthermore, decentralized platforms can hinder effective dispute resolution and enforcement.

Legally sound practices involve drafting transparent and comprehensive terms of use, clearly specifying duration, rights, and limitations of digital services, and ensuring that user rights are honoured in line with applicable European regulations. By contrast, worst practices include the use of vague or misleading contract terms, restricting access without justification, or applying pressure tactics to obtain user consent. These actions violate legal standards and compromise trust in digital platforms.

9 Copyright law

Copyright in virtual worlds is governed by international and European standards that protect intellectual creations such as software, images, music, and digital assets. Legal protection applies equally to physical and virtual works. Rights such as reproduction and public availability extend to digital environments, ensuring that creators of original content remain entitled to control how their works are used and distributed across immersive platforms.

Key principles include the requirement of individual intellectual creation, recognition of the author’s moral rights, and protection of exploitation rights. These rights are territorially bound, meaning enforcement depends on the existence of a legal connection to a specific jurisdiction. The transfer of usage rights is restricted and must be explicitly defined to ensure legal clarity and uphold the creator’s interests. In virtual spaces, this becomes especially relevant when users share or trade digital works, including NFTs and digital replicas.

Legal uncertainties arise around whether NFTs or digital twins qualify for copyright protection, and how to differentiate between original and derivative content in virtual worlds. The enforcement of rights is complicated by anonymity, decentralization, and the cross-border nature of platforms. It is often unclear whether a virtual work is sufficiently original to be protected or whether its use infringes on existing rights.

Risks include unauthorized reproduction or imitation of copyrighted content, unclear licensing terms for digital products, and the limited enforceability of rights on decentralized platforms. These risks are heightened when users mint or distribute NFTs without securing the underlying rights.

Legally sound practices involve licensing works appropriately, respecting distribution rights, and ensuring originality. Transparency in licensing and usage agreements is essential. Illegal practices include making protected content publicly available without permission, using copyrighted material in NFTs or digital twins without proper authorization, and bypassing technical protection systems. Such violations undermine legal certainty and expose actors to sanctions.

10 Criminal liability

Criminal liability in virtual worlds is governed by international and European legal standards, including the Budapest Convention on Cybercrime, the GDPR and the UN Cybercrime Treaty (adopted in 2024). These frameworks apply to virtual actions involving fraud, data manipulation, identity theft, harassment and other forms of

psychological harm, and financial crime. The attribution of liability is tied to the natural person controlling a digital avatar, meaning users are responsible for virtual actions that meet the legal criteria of a criminal offense.

Fundamental principles include personal responsibility, causality, and objective attribution of criminal acts. Virtual actions are legally assessed according to their real-world impact, particularly when harm, deception, or financial loss is involved. Jurisdictional rules based on territoriality and protective principles determine when national criminal law applies across borders. Both Europol and Interpol investigate criminal activities. Legal systems also uphold the principle of ne bis in idem to avoid duplicate prosecutions for the same offense.

Key legal challenges involve determining when avatar behaviour becomes punishable. Questions arise regarding the criminal classification of fraud involving NFTs, unauthorized cryptocurrency transactions, or manipulative digital practices. It is unclear how legal responsibility is distributed between individual users and platform operators. Another issue is cross-border enforcement when crimes span multiple jurisdictions. Security obligations for preventing offenses such as child exploitation, hate speech, or financial abuse are increasingly critical.

Major risks include phishing, fraud involving digital wallets or tokens, money laundering, and identity theft. Anonymity and decentralization heighten the danger, making it difficult to trace or prosecute offenders. Platform operators face legal risks if they fail to prevent or respond to illegal behaviour occurring on their systems. Insecure code or smart contracts can also be exploited for criminal purposes.

Best practices involve transparent and lawful handling of digital assets, compliance with privacy and security laws, and the implementation of preventive systems by platforms. Illegal conduct includes digital deception, coercion through avatars, unregulated financial activity, and the failure to address harmful or abusive content.

11 Cybersecurity

Cybersecurity in virtual worlds is governed by European regulations such as the GDPR, the NIS2 Directive, and the upcoming Cyber Resilience Act (CRA), which will introduce mandatory security standards for digital products. These frameworks apply particularly to systems that involve extended reality (XR) technologies or decentralized infrastructures like smart contracts and blockchain. Operators of platforms and digital services must ensure compliance with evolving technical and legal requirements.

Fundamental principles include the confidentiality, integrity, and availability of data and systems. These principles are also essential in immersive environments, where personal interaction, digital identities, and value transactions occur continuously. Blockchain and decentralized architectures can strengthen protection, but responsibilities must be clearly defined across system layers and platform operators. Prevention, monitoring, and user awareness are central to effective cybersecurity.

Legal challenges arise from threats such as avatar identity theft and unauthorized duplication. Ensuring secure data flows between interoperable platforms is technically complex and legally sensitive. The integrity and enforceability of smart contracts, which often trigger financial or transactional actions, are critical. XR technologies that rely on biometric data present additional legal risks, particularly when such data is misused or inadequately protected.

Main risks include unclear attribution of responsibility in the event of cyberattacks, especially when platforms interact across jurisdictions. Biometric misuse, man-in-the-room attacks, and realistic forgeries such as deepfakes are emerging threats. Insecure smart contracts or poor authentication protocols can undermine user trust and legal certainty, making robust cybersecurity essential for sustainable development of virtual worlds.

Compliant actions include the implementation of technical and organizational security measures under Article 32 GDPR, performing regular risk assessments, and applying international standards for secure authentication. Illegal practices involve collecting personal data without consent, failing to protect infrastructure, or deliberately using insecure systems. Such breaches compromise user safety and can result in regulatory penalties.

12 Data protection

Data protection in virtual worlds is primarily governed by the GDPR and related European legislation, which apply to all processing of personal data, including highly sensitive information such as biometric and behavioural data. These regulations are complemented by laws addressing privacy in digital communication and terminal equipment. A significant challenge is the international transfer of data to third countries without adequate protection, especially in decentralized systems common to Metaverse environments.

The key principles include transparency, purpose limitation, and data minimization. Users must be clearly informed about what data is collected, for what purpose, and to what extent. Only the data necessary for the intended function may be processed. When dealing with sensitive data, such as health or motion tracking, explicit consent is usually required. The right to erasure must also be upheld, although this can be difficult in persistent or blockchain-based systems.

Legal uncertainties arise around the determination of responsibility in decentralized platforms. It is often unclear who acts as the data controller when technologies such as blockchain distribute control. The enforcement of user rights like deletion and portability becomes complex across jurisdictions and technical infrastructures. The processing of biometric or emotional data in real time raises further issues, especially concerning misuse and compliance with data protection impact assessments.

Risks include the lack of accountability for data processing, excessive or opaque data collection practices, and the technical impossibility of deleting data stored immutably on blockchains. A general lack of transparency in Metaverse platforms may restrict users from exercising their legal rights effectively.

Lawful practices involve obtaining explicit consent for each data use, designing systems with privacy by design, and ensuring clear user communication. Illegal actions include processing personal data without consent, disregarding user rights to deletion or access, or misusing sensitive information without proper safeguards and authorization.

13 Design law

Design law in virtual worlds is based on European legislation such as the EU Regulation on Community Designs (CDR), which protects two- and three-dimensional designs, including virtual elements like interfaces or NFTs, as long as they are new and possess individual character. Protection can be obtained through registration, while unregistered designs enjoy limited protection for three years within the EU. International frameworks like WIPO guidelines offer additional, though sometimes limited, support in a global context.

Fundamental principles include the protectability of unique and aesthetically distinct designs, regardless of whether they are physical or virtual. Unlike trademark law, design protection does not depend on use in commerce. The aesthetic appearance alone is key, and this extends to animated or moving designs, although registering dynamic visuals remains technically challenging. The principle of territoriality limits protection to the jurisdiction in which the design is registered.

Key legal issues in virtual worlds involve the registrability of dynamic digital objects, which are only partially covered by current systems. The territorial scope of protection becomes problematic when virtual platforms operate globally. Furthermore, enforcing design rights is increasingly difficult in decentralized and often anonymous environments, such as blockchain-based networks, where identifying infringers is not straightforward.

Main legal risks include the unauthorized use of protected designs by unknown users, the limited enforceability of rights outside registered regions, and the inadequate legal protection for animated or interactive virtual designs due to technical constraints. These challenges can lead to significant losses for creators if infringements remain unaddressed.

Lawful conduct includes registering designs in line with legal requirements, respecting designer rights in licensing and use, and utilizing platform mechanisms to flag infringing content. Illegal practices involve reproducing or altering protected designs without permission, using designs without proper registration, and commercially

exploiting third-party creations without disclosure or consent. Such actions undermine legal protections and expose violators to sanctions.

14 Digital identities

Digital identities in virtual worlds are regulated by various European legal frameworks, with the eIDAS Regulation (Regulation EU No. 910/2014) and the upcoming eIDAS 2.0 reform playing a central role. These aim to standardize digital identification and establish a European digital identity wallet. Additional rules address data protection, anonymity, and the management of identification data, especially in cross-border or sensitive sectors such as finance or online gaming. Digital Markets Act (DMA) provisions may apply when digital identity usage intersects with platform regulation across jurisdictions.

The core principles guiding digital identity systems are legality, purpose limitation, and data minimization, as outlined in the GDPR. Users should only share the information required for specific use cases, and systems must prioritize anonymity or pseudonymity wherever legally permissible. Where identification is required—such as for financial services—the know-your-customer (KYC) principle must be properly implemented. The creation of uniform standards, particularly through the EUid wallet, is intended to ensure consistency, interoperability, and enhanced security across platforms.

Central legal challenges include balancing privacy with secure authentication. Legal questions arise as to when pseudonyms suffice and when real-name identification is mandatory. Platform interoperability requires reliable identity assignment across virtual environments. Additionally, legal certainty must be ensured in identity verification processes involving blockchain or video identification, while also resolving conflicts between privacy and identification obligations, especially in regulated sectors.

Risks include breaches of data protection due to improper storage or sharing of identity data, insufficient authentication mechanisms that allow identity theft, and unclear responsibilities between users, platforms, and third-party verifiers. Fragmented standards and weak technical infrastructure further complicate compliance and user protection.

Legally compliant behaviour includes transparent identity management, adherence to KYC rules, use of secure verification technologies, and alignment with the eIDAS framework. Illegal practices involve unauthorized processing, mandatory real-name use without legal basis, poor security, or failure to meet interoperability and standardization obligations.

15 Fair trade

Fair trading law in virtual worlds is governed by European principles protecting against unfair business practices, particularly in the context of digital and immersive environments. The legal framework prohibits deceptive or obstructive conduct and extends to new advertising formats such as AR and location-based targeting. These technologies raise specific legal questions in virtual spaces, especially when they influence user perception or restrict market access for competitors.

The core principles include maintaining fair competition, preventing misleading or aggressive commercial practices, and ensuring that advertising is not used to obstruct rivals or manipulate consumers. In immersive contexts, contextual advertising must respect the boundaries of fair conduct, avoiding techniques that intentionally distort user choice or restrict visibility for other providers. Public perception and evolving digital norms also play a role in assessing what constitutes unfairness in new formats.

Priority legal questions include whether location-based or AR-driven advertisements amount to manipulation, how to distinguish between fair promotion and illegal solicitation, and to what extent platform operators bear responsibility for actions taken by third parties within their ecosystems. These issues are further complicated by differing international legal interpretations, especially for global platforms operating across jurisdictions.

Risks arise when advertising strategies create technical or visual barriers for competitors or when they mislead consumers through unclear presentation or undisclosed promotional content. Platform operators may also face liability for failing to prevent unfair practices by users or advertisers within their virtual environments. These risks can lead to warnings, reputational damage, or regulatory sanctions.

Compliant behaviour includes clear labelling of advertising, non-discriminatory presentation of content, and adherence to information obligations. Fair use of AR is permitted when it enhances rather than manipulates user experience. Illegal conduct includes covertly influencing consumer decisions, hiding the commercial nature of content, or unfairly limiting competitor access, all of which can trigger legal consequences and erode trust.

16 Financial supervisory law

Financial supervisory law in virtual worlds is governed by national and European regulatory frameworks, including the Markets in Crypto-Assets Regulation (MiCA) and the Second Payment Services Directive (PSD2). These laws set requirements for licensing, capital adequacy, and risk management for financial service providers, particularly in relation to payment systems, crypto assets, and digital financial platforms. They are designed to ensure that financial activities, even within virtual environments, meet standards for market stability and consumer protection.

Core principles include transparency in operations, protection of users from financial harm, and the integrity of digital markets. Financial services offered in virtual worlds must be clearly structured within a legal framework that allows oversight and enforcement. The territoriality principle and the target market approach guide the applicability of national laws to cross-border services. The digital nature of virtual economies demands new mechanisms for secure identification and transaction traceability.

Key legal issues include the regulation of decentralized financial systems (DeFi), including stablecoins and smart contracts, which challenge traditional financial oversight. Compliance with anti-money laundering rules in anonymous or pseudonymous environments presents another major concern. It is also unclear how conventional supervisory principles apply to innovative digital assets and services, particularly in the context of international transactions and decentralized ecosystems.

Legal risks include the unregulated issuance or trade of crypto tokens, inadequate transparency in financial operations, and violations of money laundering laws due to anonymity. The absence of clearly defined responsibilities on decentralized platforms increases uncertainty and regulatory gaps.

Best practices involve obtaining proper licenses, complying with KYC and AML regulations, and registering financial activities in accordance with MiCAR standards. Transparent documentation and internal compliance procedures help ensure legal certainty. Illegal practices include unauthorized issuance of crypto assets, avoiding identity checks, and spreading misleading financial information. Such actions can result in heavy sanctions and regulatory intervention.

17 Financial transactions

Financial transactions in virtual worlds are regulated under European frameworks such as the Markets in Crypto-Assets Regulation (MiCA) and the EU Anti-Money Laundering Directive. These laws apply to activities involving cryptocurrencies, NFTs, and digital assets, which are often classified as e-money or financial instruments depending on their structure and function. Financial services offered in virtual environments must comply with applicable supervisory and licensing requirements, especially when they involve payments or asset trading across borders.

The key principles are transparency, traceability, and transaction security. These ensure consumer protection and help prevent financial crimes such as money laundering or fraud. Service providers must implement strong authentication and data security systems to protect the integrity of financial processes. Even in global virtual settings, the territorial principle remains relevant for determining which regulatory framework applies to specific transactions.

Legal challenges include classifying virtual currencies and NFTs within existing financial law, ensuring compliance with anti-money laundering regulations in decentralized networks, and managing the legal complexity of cross-border transactions. Another critical issue is the interoperability of platforms and how payment systems can be legally and technically integrated into virtual environments.

Legal risks arise from the vague classification of digital assets, which creates regulatory uncertainty. Decentralized systems often lack transaction traceability, increasing the potential for fraud or illicit transfers. Liability concerns also emerge when technical failures or security breaches occur within platforms providing financial services or handling digital assets.

Legally compliant behaviour includes obtaining the necessary authorizations, applying strong know-your-customer controls, and transparently informing users of transaction risks and fees. The use of approved technologies and licensed platforms helps to reduce compliance risk. Illegal practices include unlicensed financial activity, lack of identity verification, and deceptive communication regarding transaction terms. Fraudulent use or manipulation of payment systems also constitutes a breach of financial regulations and can result in sanctions.

18 Gambling law

Gambling law in virtual worlds is shaped by national and international frameworks that regulate the offering, mediation, and advertising of games of chance. While terrestrial and online gambling are well defined in current legislation, virtual worlds introduce a hybrid form that complicates legal classification. European data protection and digital service regulations, such as the GDPR and upcoming information society provisions, may also impact how gambling platforms operate. Challenges arise especially when applying traditional licensing and monitoring rules to decentralized and immersive environments.

The fundamental principles include the protection of players and minors, the prevention of addiction, and the guarantee of transparency and fairness. Gambling is generally prohibited unless explicitly authorized, based on a preventive control system. The principle of channelling aims to steer users toward legal, monitored offers to reduce illegal market activity. Identification requirements, behavioural monitoring, and loss limitation mechanisms are central to responsible gambling practices.

Key legal issues focus on how to define gambling in virtual worlds. It remains unclear whether these activities fall under existing internet gambling laws or require a new legal category. Anonymity in virtual environments raises concerns about verifying user identity and age, particularly for youth protection and anti-money laundering compliance. Additionally, the enforcement of current technical requirements, such as exclusion registers or loss caps, is problematic. New forms of gaming, such as avatar-based competitions or AI-driven betting, further complicate regulatory alignment.

Risks include the growth of illegal markets due to insufficient control, the circumvention of protection measures, and manipulation through AI-targeted advertising. Weaknesses in crypto-based payment systems may also lead to regulatory breaches. The classification of novel gaming formats remains a legal grey area.

Lawful conduct includes obtaining licenses, implementing identification mechanisms, and applying protective tools within virtual settings. Illegal practices involve unauthorized gambling offers, use of unregulated cryptocurrencies, targeting of vulnerable groups, and failure to comply with existing advertising and transaction standards.

19 Gaming and eSports

There is some uncertainty about standardisation of rules with respect to real-world rules, however, it is generally agreed that gaming and eSports in virtual worlds are governed by a mix of national and international legal frameworks. At the European level, the Markets in Crypto-Assets Regulation (MiCAR) and the eIDAS Regulation are central, particularly when dealing with authentication, in-game currencies, and NFTs. Data protection is also crucial, with the General Data Protection Regulation (GDPR) applying to all user data collected during gameplay. Contracts involving digital content and consumer rights also influence how platforms operate and deliver services across borders.

Core principles include the protection of minors and consumers, fairness in competition, and transparency in in-game systems. There is lack of clarity regarding legal status of doping in eSports, however, these could be included or added when clear benchmarks and rules for the treatment of the players are defined.

In-game purchases and loot boxes must be clearly disclosed and assessed for potential gambling elements. Data must be processed according to purpose limitation and transparency standards. Where financial transactions occur, the know-your-customer (KYC) principle is important. In eSports, fair competition and equal opportunity are key, especially in determining whether VR-based activities meet sport recognition criteria. Content harmful to young people must be restricted through technical and organizational controls.

Legal uncertainties include the classification of loot boxes, which may fall under gambling regulation, and the legal handling of NFT and cryptocurrency trading within games. The treatment of "play-to-earn" models and the criteria for recognizing eSports as sport in the context of VR technologies also require further legal clarity. Platform operators must understand their obligations to manage content, data, and user behaviour appropriately.

Legal risks include the misuse of data, unauthorized trading of digital assets, lack of protection for minors, and insufficient transparency in monetization models. Cross-border enforcement remains difficult due to jurisdictional fragmentation. Security vulnerabilities in blockchain-based systems pose further risks.

Legally compliant behaviour involves transparent game mechanics, protective measures for minors, and full adherence to data and financial regulations. Unlawful actions include offering loot boxes without regulatory checks, disclosing personal data without consent, and neglecting age restrictions or platform security standards.

20 Insurance law

Insurance law in virtual worlds is governed by general contract and supervisory regulations, supplemented by European laws such as the General Data Protection Regulation (GDPR). These frameworks apply to insurers operating within virtual environments, especially when handling personal data or offering cyber risk coverage. The emerging relevance of the EU AI Regulation also affects insurers using AI technologies for automated processes or virtual claims management. Insurers must adapt traditional frameworks to the digital realities of virtual worlds, including the insurability of virtual assets. It is unclear how fractional ownership in virtual worlds fits into insurance.

Fundamental principles include transparency, fairness, and security in contract execution and claims processing. Insurers must provide clear risk assessments and ensure that policyholders can access services without technical or legal obstacles. Cyber insurance is expected to cover risks such as data loss, hacking, or manipulation. Data minimization and the responsible handling of personal information are especially critical in immersive, identity-driven environments where personal and behavioural data is constantly generated.

Key legal questions concern the coverage of virtual assets like NFTs or digital twins, and whether existing products are sufficient to insure risks such as cyberattacks or virtual property damage. The use of AI systems must comply with transparency obligations and data protection laws. It must also be clarified how policyholder identity is verified in decentralized systems and how to apply existing regulations to claims arising from non-physical damages.

Risks include legal uncertainty about whether and how virtual objects are insurable. Ambiguities in policy terms, weak contract design, and a lack of transparency in AI use may cause legal conflicts or consumer mistrust. Data breaches involving VR systems or inadequate claims procedures in virtual environments also pose compliance challenges.

Legally compliant behaviour involves transparent policy terms, coverage of virtual risks, and strict adherence to data protection standards. Illegal practices include unclear contract conditions, non-consensual data processing, and insufficient coverage of foreseeable digital risks within virtual worlds.

21 Intellectual property

Intellectual property in virtual worlds is regulated by established systems of copyright, trademark, and industrial property law, alongside international agreements such as TRIPS and relevant EU legislation. These frameworks

apply to both existing works and newly-created content or trademarks transferred into virtual environments. Digital assets in virtual worlds must be evaluated under these laws, even though the application of territorial rules becomes increasingly complex in globally-accessible, decentralized platforms.

Core principles include the requirement of originality and sufficient creative input for copyright protection, and the principle of territoriality, meaning that rights only apply within defined jurisdictions. Trademark protection requires actual use in commerce, which also applies in the virtual world when digital branding has a commercial function. Rights holders must enforce their claims actively, as protection is not automatic against all virtual infringements.

Legal challenges primarily concern enforcing property rights in an environment that transcends territorial limits. Key issues include whether existing laws are adaptable to virtual objects and how trademark use in virtual worlds can be effectively demonstrated. Responsibility is also blurred in decentralized structures where no single platform operator exists, raising the question of liability for user-generated infringements and the limits of enforcement.

Legal risks include widespread copying and manipulation of copyrighted content, difficulties in blocking infringing materials, and users or platforms bypassing regional restrictions. Without effective digital enforcement tools, rights holders may struggle to prevent the unauthorized distribution or imitation of their intellectual property.

Compliant behaviour involves using protected content only with authorization, registering trademarks and designs for virtual applications, and clearly licensing rights with transparent compensation. Illegal practices include unlicensed reproduction, trademark imitation, and circumvention of digital protection systems. Manipulating protected designs to deceive or avoid detection is also unlawful and undermines the enforceability of intellectual property rights in virtual spaces.

22 Labour law

Labour law in virtual worlds is governed by existing national and European regulations, particularly in relation to working conditions, data protection, and co-determination. While no specific international framework addresses virtual work environments, general labour standards still apply. This includes rules on working hours, occupational safety, and the protection of personal data. The GDPR plays a central role in regulating the handling of sensitive data generated through VR or AR technologies. Employee representation must also be involved when introducing new digital tools or altering working environments.

Fundamental principles include the employer’s duty of care, which requires ensuring both physical and psychological safety, even in virtual spaces. Employers may exercise managerial authority regarding time, location, and type of work, but only within reasonable limits. Transparency and proportionality are essential when processing employee data. Additionally, any implementation of new immersive environments and tools must respect the co-determination rights of employee representatives to protect staff interests.

Key legal issues include how to ensure safety and legal compliance in immersive and interactive workplaces, how to prevent the blurring of boundaries between work and personal time in flexible models, and how to manage the extensive data generated by virtual environments. There are also considerations over what territory someone is working in if this is only being carried out in an immersive environment. The territory in which the work is done impacts which laws apply, right to work / immigration and taxes. Performance evaluations based on such data raise additional concerns about transparency, fairness, and privacy.

Legal risks include breaches of data protection due to excessive or unauthorized surveillance, as well as health risks from prolonged use of immersive technologies. There is also a risk of labour law violations if virtual work leads to continuous availability without defined working hours or rest periods, blurring the lines between professional and private life.

Compliant practices involve conducting health risk assessments, implementing respectful behavioural guidelines for virtual interaction, and ensuring transparency in data usage. Illegal practices include unjustified surveillance, mandatory Metaverse use without agreement, and violating working time laws through undefined hours or excessive demands, all of which can lead to legal consequences.

23 Lawyers' professional law

Lawyers' professional conduct in virtual worlds is governed by traditional legal frameworks, with additional relevance from international instruments like the Rome I Regulation and the General Data Protection Regulation (GDPR). Legal services provided in virtual environments are subject to the same principles as in physical settings, though digital contexts introduce new challenges. Platform terms and conditions may affect contractual obligations, especially when legal services are delivered via avatars or within decentralized systems.

Fundamental principles remain unchanged. Confidentiality between lawyer and client is paramount and must be technically safeguarded in virtual environments. Independence in legal practice must be maintained regardless of platform structures. The Rome I Regulation secures party autonomy in cross-border agreements, ensuring freedom in choosing applicable law. Authentication of clients and lawyers is necessary to validate digital transactions and prevent misuse. Transparency in contract design, including jurisdiction clauses, remains a core requirement.

Legal questions centre on how to ensure secure and verifiable client authentication in avatar-based interactions, how to apply conflict-of-law rules to cross-border mandates, and whether smart contracts meet legal standards. Lawyers must also determine how to fulfil their professional obligations in a platform-controlled ecosystem and how digital legal activities, such as remote representation, align with procedural laws.

Risks include data leaks due to insufficient encryption or poor identity verification. Sensitive information, including biometric data, is exposed in immersive environments, increasing the likelihood of breaches. Disputes may arise over applicable law in international mandates. Failure to meet formal contract requirements, such as for real estate transactions, adds further legal uncertainty. There is also the risk of conflict with platform operators over enforcement of client rights.

Best practices include secure identity verification, proper contract drafting under Rome I, and legally sound smart contract integration. Unlawful actions involve breaches of confidentiality, unauthorized legal practice, mishandling of personal data, and invalid contractual procedures, all of which may result in sanctions or loss of legal validity.

24 Legal protection and jurisdiction

Legal protection and jurisdiction in virtual worlds are governed by national procedural rules and European instruments such as the Brussels Ia. Regulation, which defines international jurisdiction. Cross-border dispute resolution is also influenced by international conventions like the New York Convention, particularly regarding the recognition and enforcement of arbitral awards. As legal disputes increasingly involve digital goods and virtual interactions, regulations concerning online arbitration and smart contracts will become essential.

The core principles include procedural fairness, effective access to justice, and enforceable dispute resolution. The global nature of virtual platforms challenges the principle of territoriality, raising complex jurisdictional questions. Party autonomy remains central, especially when designating jurisdiction or agreeing to arbitration forums. Additionally, legal systems must address the risk of abuse through anonymity by requiring some form of identifiability from participants in legal processes.

Legal challenges include determining jurisdiction in disputes involving anonymous users or virtual assets like NFTs. The enforcement of smart contracts and the admissibility of digital evidence in legal proceedings are pressing questions. Enforcement of judgments or arbitral decisions is especially difficult when parties are pseudonymous or assets exist only in digital form. It is also unclear to what extent online arbitration, including blockchain-based mechanisms, meets legal standards for dispute resolution.

Risks involve uncertainties in establishing which court has jurisdiction when platforms span multiple legal territories. Anonymity complicates legal enforcement, making it difficult to identify or hold parties accountable. Enforcing decisions involving digital assets poses challenges, especially where asset ownership is difficult to trace. The legal status of smart contract outcomes and digital arbitration awards remains unclear in many jurisdictions.

Best practices include defining jurisdiction and arbitration clauses clearly in contracts, ensuring online dispute processes meet legal standards, and integrating smart contracts only when transparency and traceability are

guaranteed. Platforms may implement dispute resolution frameworks in their terms, provided these do not override mandatory legal protections.

25 Media law

Media law in virtual worlds is shaped by various national and European regulations that apply to digital content, platform responsibilities, and user protection. At the European level, the General Data Protection Regulation (GDPR), the E-Commerce Directive, and the Audiovisual Media Services Directive (AVMSD) are particularly relevant. These laws govern issues such as content moderation, age restrictions, and cross-border distribution of media. The principle of the country of origin and conflict of laws rules are central to determining regulatory authority in a global virtual environment.

Core principles include the protection of minors from harmful content, the safeguarding of human dignity, and the prohibition of criminal material such as child pornography or depictions of violence. Freedom of expression remains a protected right within the limits of legal boundaries. Self-regulation allows platforms to implement voluntary compliance through recognized bodies and develop internal mechanisms for content moderation. Technological neutrality ensures that evolving formats like virtual reality are covered under existing frameworks without needing entirely new legislation.

Legal questions focus on how to assess and regulate immersive experience content, the design and enforcement of age verification systems, and the extent of platform liability for user-generated content. The classification of in-game advertising and monetization mechanisms like loot boxes raises concerns, as does the use of artificial intelligence in automated content moderation. The challenge of applying the country of origin principle in a borderless virtual world also complicates enforcement responsibilities.

Legal risks include the dissemination of illegal content, failure to implement adequate youth protection mechanisms, and non-compliance with national content standards. Weak data protection practices and ineffective moderation can lead to sanctions or service restrictions.

Compliant platforms employ robust age verification, content labelling, and youth protection protocols, and adhere to transparency and privacy standards. Illegal practices involve the unregulated distribution of harmful content, neglect of age restrictions, and failure to address harassment or abuse effectively within virtual communities.

26 Medical and medical device law

Medical and medical device law in virtual worlds is governed by European regulations, particularly the Medical Device Regulation (MDR, EU 2017/745), which outlines requirements for safety, performance, and classification. Rule 11 of the MDR is especially relevant for software-based applications. Data protection standards such as the General Data Protection Regulation (GDPR) also apply, particularly for the processing of sensitive health data. Cross-border use of medical technologies may additionally fall under international frameworks like those of the FDA or similar regulatory authorities in other jurisdictions.

The fundamental principles include patient safety, transparency, and validated efficacy. All products must be used in accordance with their intended purpose and undergo appropriate risk classification and conformity assessment. Software must be rigorously evaluated, especially when it contributes to diagnosis or therapy. Ensuring data protection and avoiding misinformation are central to market authorization and public trust.

Key legal issues relate to defining whether virtual tools such as virtual world-based therapies, digital twins, or virtual simulations qualify as medical devices. Questions arise regarding the classification and approval procedures for these tools, especially when used in areas like surgery training or psychological therapy. Liability concerns emerge when digital interventions lead to incorrect diagnoses or treatment outcomes. Additionally, the processing of sensitive health data through immersive or AI-driven technologies poses challenges for lawful data handling.

Legal risks include misclassification of medical devices as non-regulated lifestyle products, inadequate testing, and failure to meet safety standards. Data breaches in the use of AI tools or immersive health platforms can result in

serious legal consequences. Poor integration of hardware, such as wearable displays, into safety evaluations further increases regulatory vulnerabilities.

Legally-compliant practices involve full certification under MDR, secure telemedicine applications, correct classification of software, and lawful data processing. Illegal conduct includes unauthorized product use, misleading medical claims, and attempts to bypass regulation by rebranding devices as lifestyle tools.

27 Patent law

Patent law in virtual worlds is governed by national and international frameworks, including the European Patent Convention (EPC), which defines the requirements for the protection of technical inventions. Articles 52 et seq. EPC are particularly relevant for determining what constitutes a patentable invention. Software, algorithms, VR hardware, blockchain applications, and data sequences may be protected if they demonstrate a technical solution to a technical problem. The guidelines of the European Patent Office (EPO) provide further clarity, especially concerning computer-implemented inventions.

Core principles include technicality, novelty, inventive step, and industrial applicability. Patent protection is only granted to inventions that achieve a specific technical effect. While computer programs are generally excluded, they can be patentable if they go beyond normal data processing and result in an additional technical contribution. Data sequences may also be protected if directly derived from a patented technical process. In virtual worlds, these principles extend to complex digital environments and emerging technologies like virtual reality and blockchain.

Key legal questions include whether digital representations, such as avatars or simulated environments, qualify as technical inventions. The classification of algorithms and virtual simulations within patent law is also debated, especially when these tools are used to perform or replicate real-world functions. Another challenge is the enforcement of patent rights in virtual worlds, where virtual replicas of protected technologies may be offered or used without authorization.

Legal risks include the unauthorized use of patented elements in virtual products, the ambiguous classification of software-based inventions, and difficulties in enforcement due to the international structure of virtual world platforms. There is also risk in granting patents to innovations lacking technical substance, which can lead to uncertainty and disputes.

Lawful practices include licensing protected technologies, developing software with genuine technical effects, and offering virtual products that do not infringe existing patents. Infringement occurs through unauthorized replication, misleading patent filings, or commercial use of unlicensed patented processes or outputs.

28 Police law and state control

Police law and state control in virtual worlds are shaped by national regulations and supplemented by European and international standards. The Data Protection Directive for Justice and Home Affairs, the General Data Protection Regulation (GDPR), and the European Convention on Human Rights (ECHR) provide legal boundaries for state intervention. With the growing role of artificial intelligence in virtual policing, future regulations such as the proposed EU AI Regulation are becoming increasingly relevant. National criminal procedure codes remain central for actions relating to investigation and enforcement.

Key principles include the proportionality of police measures, requiring that any interference with fundamental rights be suitable, necessary, and balanced. In virtual worlds, this applies particularly to surveillance, data collection, and virtual identity monitoring. The legal distinction between preventive measures and criminal prosecution remains crucial. Additionally, international principles prohibit discrimination and safeguard freedom of expression, even in digital environments.

Major legal challenges include defining lawful actions by state authorities within decentralized platforms, clarifying the legitimacy of police avatars and AI-based tools, and determining jurisdiction in cases of cross-border criminal activity. The role of private platforms in supporting or executing state measures also raises legal and ethical

questions. The regulation of novel criminal behaviour in virtual environments, such as fraud involving NFTs, demands new legal interpretations.

Legal risks involve unclear jurisdictional boundaries, unregulated use of AI systems for surveillance, and violations of data protection norms. If police actions rely on opaque algorithms or store personal data without justification, significant legal consequences may follow. Weak technical security in state-operated systems also exposes operations to misuse or cyberattacks.

Best practices include ensuring transparency and legal authorization for all police actions, using AI within regulatory limits, and cooperating with platforms under clear legal frameworks. Unlawful conduct includes disproportionate surveillance, unregulated AI use, international overreach, and covert actions without explicit legal basis.

29 Private international law

Private international law in virtual worlds is governed by multiple legal frameworks, including the Rome I Regulation for contractual obligations and the Rome II Regulation for non-contractual claims. The UN Convention on Contracts for the International Sale of Goods (CISG) applies to international goods transactions, while jurisdiction is often established through the Brussels Ia Regulation and, where applicable, the Hague Convention on Jurisdiction. These instruments are essential in virtual environments where cross-border interactions dominate. Conflict-of-law rules gain prominence in virtual worlds due to the global, decentralized nature of digital platforms.

Core principles include party autonomy, which allows contracting parties to choose the applicable law, and the principle of closest connection, which assigns law based on the strongest factual link. Further principles focus on the protection of weaker parties, such as consumers or employees, as well as legal certainty and predictability in international commerce. Within the EU, mutual recognition plays a vital role in ensuring legal consistency across borders.

Key legal questions include determining applicable law when users interact anonymously or via avatars, and clarifying which legal system governs digital transactions involving NFTs or cryptocurrencies. Enforcement is further complicated when contracts are concluded without physical presence. Other issues include consumer protection in virtual contracts and the effectiveness of data protection regulations in a global setting.

Main risks involve uncertainty about applicable law and jurisdiction, particularly when users conceal their identity. There is also a risk that dominant platforms use choice-of-law clauses to bypass consumer rights. Smart contracts and blockchain-based interactions can conflict with legal norms, especially when lacking dispute resolution mechanisms. The lack of harmonization across legal systems reduces overall legal certainty.

Legally compliant actions include the transparent application of choice-of-law clauses, respect for consumer rights, and the implementation of smart contracts with built-in safeguards. Unlawful conduct includes misleading choice-of-law terms, disregard for mandatory legal protections, and automated processes that neglect essential legal standards.

30 Right of personality

Personal rights in virtual worlds are protected by national laws and European frameworks such as the General Data Protection Regulation (GDPR). These regulations ensure the safeguarding of personal dignity, privacy, and data. Conflict-of-law rules like the Rome II Regulation determine jurisdiction in cases involving cross-border infringements. In virtual environments, platform terms of use and international standards further influence the protection and exercise of personal rights.

Fundamental principles include the right to privacy, informational self-determination, and the free development of personality. These principles extend to digital spaces, covering the use of avatars, biometric data, and personal characteristics. Individuals have the right to control how their digital likeness is used, particularly regarding

commercial exploitation. The balance between freedom of expression and the protection of dignity is especially relevant in online settings where content spreads rapidly and anonymously.

Central legal questions include the extent to which avatars are legally protected as personal representations and what rights users have if their digital identity is manipulated, copied, or misused. Other concerns involve the lawful collection and use of personal data by platform operators and the boundaries between acceptable expression and harassment. Questions also arise concerning the post-mortem right of personality and how digital legacies are managed after a user's death.

Legal risks involve unauthorized use of avatars, identity theft, and misuse of personal data. Users may suffer reputational harm or psychological distress if their digital presence is exploited or defamed. Jurisdictional uncertainties can hinder enforcement, especially when platform operators are based abroad. Platform terms that override basic personal rights may be legally questionable.

Compliant practices include respecting user consent, protecting data in line with the GDPR, and implementing anti-harassment tools. Illegal conduct includes the commercial use of avatars without permission, defamation, and lack of protective mechanisms by platforms. Failing to uphold personal rights in digital spaces may result in significant legal consequences.

31 Supply Chain Act

The Supply Chain Due Diligence Act (LkSG), effective since 2023 in Germany, imposes obligations on large companies to identify and mitigate human rights and environmental risks throughout their supply chains. These obligations apply to both direct operations and relationships with suppliers. Although originally focused on physical goods and services, the law's principles are increasingly relevant in digital contexts such as virtual worlds. Here, civil law and applicable international regulations also govern how due diligence responsibilities translate into virtual supply chain structures.

The guiding principles of the LkSG include prevention, risk minimization, and the duty of care. Companies must assess risks not only within their own operations but also among upstream and downstream partners. Appropriateness is a key factor, requiring companies to take reasonable measures based on their influence and position within the supply chain. In virtual environments, these principles must adapt to the decentralized and often anonymous nature of business relationships.

Legal uncertainties arise around whether digital products like NFTs or services provided in virtual worlds fall under the LkSG definition of a supply chain. Questions also surround the role of platform operators in the context of legal accountability. Identifying human rights or environmental risks is particularly challenging when actors operate without clear identities or central governance structures.

Risks include the inability to trace suppliers or partners, making proper risk analysis and preventive action nearly impossible. DAOs further complicate compliance due to their decentralized nature. Companies that fail to meet due diligence standards may face fines or exclusion from public tenders.

Legally compliant actions include conducting risk analyses, documenting due diligence efforts, and incorporating human rights clauses into digital supply agreements. Unlawful practices include ignoring known risks, engaging with anonymous entities without vetting, and omitting contractual safeguards that address environmental and human

32 Tax law

Tax law in virtual worlds is governed by national and international regulations that apply to digital activities and virtual assets. These include rules for income taxation, corporate taxation, and value-added tax. Income generated from the use of cryptocurrencies or NFTs can be classified differently depending on whether it stems from private sales, business activity, or investment. Transactions in virtual environments, such as the sale of NFTs or leasing of virtual property, may also fall under value-added tax obligations, though their tax treatment remains complex and evolving.

Core principles include the global income principle, which subjects worldwide income to taxation in the taxpayer's country of residence, and the ability-to-pay principle, which ensures taxes are proportionate to an individual's financial situation. Additionally, the concept of economic transactions, including the exchange of digital services or goods, is key to determining tax liability, particularly for indirect taxes like value-added tax.

Legal uncertainties arise around how to classify income generated within virtual environments, how to treat virtual currencies when converted into fiat money, and how double taxation agreements apply to cross-border transactions involving decentralized platforms. The use of anonymous digital wallets and decentralized financial systems complicates the identification and documentation of taxable events.

Major risks include incorrect or missing classification of taxable transactions, potential tax evasion through untraceable platforms, and uncertainty about value-added tax obligations for digital goods. These issues are exacerbated by the speed of technological development, which outpaces legal clarity.

Compliant behaviour includes declaring all income accurately, applying value-added tax correctly to virtual sales, maintaining proper documentation, and adhering to transparency and identification rules in transactions. Unlawful conduct includes hiding income, failing to report value-added tax, or using offshore structures to evade tax. Such violations can result in significant financial penalties and reputational damage.

33 Tenancy and residential property

Tenancy and residential property law in virtual worlds is governed by digital contract regulations, notably those established under the EU Digital Content Directive. Virtual properties, including NFTs representing land or real estate, are treated as digital products rather than physical objects. As such, traditional property law does not apply directly. Instead, these assets are interpreted as license rights, meaning that their legal treatment focuses on contractual obligations and digital service standards rather than ownership in the classical sense.

Fundamental principles include the principle of equivalence, which ensures that the value of the digital lease corresponds to the agreed consideration. Tenancy rules are applied analogously, granting users certain rights such as the ability to reduce or terminate usage in case of defects. The territoriality principle plays a minor role, as the global nature of virtual worlds limits the relevance of national borders in contractual relationships.

Legal uncertainties arise concerning the status and enforceability of digital tenancy agreements, particularly in defining rights and remedies for defects such as access interruptions, software failures, or usability issues. It must be clarified whether traditional tenancy or purchase regulations can be applied, and how license-based arrangements are interpreted in the context of digital property.

Key risks involve ambiguous liability for service outages, platform dependencies that compromise stability, and vague license agreements that may allow manipulation or misuse. Enforcement is complicated by jurisdictional fragmentation across global digital platforms.

Legally compliant behaviour includes structuring contracts according to digital contract law, clearly defining user rights and obligations, and maintaining usability through technical support and transparency. Unlawful actions involve unclear or misleading license terms, unjustified restrictions on user rights, and failure to provide remedies for non-performance. Concealing the true nature or use of virtual property may also trigger legal consequences.

34 Trademarks

Trademark law in virtual worlds is governed by national and European frameworks, particularly the European Union Trademark Regulation, which provides harmonized rules for protecting trademarks in both physical and digital contexts. The World Intellectual Property Organization (WIPO) Nice Classifications, including the updates to Class 9 that went into effect in 2024, also reflect global policies with respect to virtual goods and services, including those linked to NFTs. However, due to the territoriality principle, trademark protection is geographically limited, requiring companies active in global virtual spaces to seek multiple registrations in relevant jurisdictions to ensure comprehensive protection.

Fundamental principles include safeguarding distinctiveness, ensuring a trademark identifies the origin of goods or services, and preventing consumer confusion. Trademarks must not be used merely decoratively or descriptively. In virtual environments, including those involving NFTs or digital products, the same criteria apply, though additional clarity is needed to specify the scope of digital trademark use. Virtual trademarks must be clearly linked to a provider to avoid ambiguity in enforcement.

Key legal issues include whether virtual trademarks are independently protectable, how to differentiate between virtual and real-world goods when assessing confusion, and how to enforce rights in decentralized or anonymous environments. As platforms often lack centralized control, monitoring and preventing misuse becomes complex, especially when user identities are hidden.

Risks include inconsistent legal recognition of trademarks across jurisdictions, leading to difficulties in cross-border enforcement. There is also a heightened risk of misuse, such as counterfeit NFTs using established brand identifiers. Platform operators may face liability if they do not act against clear infringements.

Compliant practices include proper registration of trademarks for digital goods, adherence to trademark use requirements, and transparent licensing arrangements. Establishing clear internal policies for virtual trademark use supports legal clarity. Unlawful conduct includes unauthorized use of protected marks, registering trademarks in bad faith, and exploiting territorial limitations to use protected marks in regions without registration. Such acts can result in infringement claims and legal penalties.

35 Use of standards: legal implications

The legal use of standards in virtual worlds is shaped by national and European regulations concerning product safety, liability, and consumer protection. While technical norms such as ISO or DIN standards are not binding laws, they represent the recognized state of the art and are critical in assessing whether a product meets legal safety and quality requirements. European regulations such as Regulation (EU) 2019/1020 on market surveillance and the General Data Protection Regulation (GDPR) also influence how digital and physical virtual world products are assessed and brought to market.

The core principles are product safety, duty of care, transparency, and the protection of consumers. Manufacturers and developers must ensure that their products do not pose foreseeable risks. The obligation to meet safety standards applies not only to physical goods such as VR equipment but also to digital offerings like immersive software or AI-driven environments. Compliance with established norms helps to demonstrate legal diligence and reduces liability risks.

Key legal questions include how to apply traditional product safety and quality standards to virtual or hybrid products, especially those used in immersive environments. Standards for interoperability, algorithmic transparency, and data security play a crucial role in determining lawful product development. The challenge lies in adapting global standards such as ISO 27001 to emerging virtual worlds and ensuring legal accountability for safety or data breaches across jurisdictions.

Legal risks include liability for damages if a product is deemed defective due to non-compliance with established technical standards. In digital settings, using unsafe code, non-compliant data processing, or misleading consumers about product features can trigger both civil and regulatory consequences.

Lawful conduct involves designing products in line with safety and data protection norms, disclosing risks transparently, and adopting international standards voluntarily. Illegal conduct includes releasing unsafe or deceptive products, neglecting data protection standards, and ignoring user safety obligations in either hardware or software components.

36 Conclusion

36.1 Overview

Classical legal doctrines, such as contract law, company law, consumer protection, and intellectual property law, offer crucial continuity and legal certainty in virtual worlds. These legal frameworks ensure that agreements between users and platforms, or between avatars and businesses, are enforceable under familiar principles. Contract law supports the enforceability of smart contracts, while consumer law anchors rights like withdrawal, warranty, and redress in digital-only transactions.

Company law plays a stabilizing role by defining liability structures and governance expectations, which is particularly relevant as novel entities like DAOs emerge. IP law, including copyright and trademark, protects creative output in virtual economies, whether or not it be digital art, avatars, or branded spaces. In this context, standardised practices (e.g. licensing formats, rights metadata) provide legal clarity and facilitate enforcement.

Design law and data protection law further protect users and creators by safeguarding digital designs and personal identity representations. Where such legal frameworks are applied effectively, they provide a strong normative structure for dispute resolution, civil liability, and market participation in virtual worlds.

The legal frameworks should always be consistent and, where possible be referenced in the European Commission's eight values and principles, as defined in the Virtual Worlds Toolbox: freedom of choice, sustainability, human-centered approach, health, education, safety and security, transparency and inclusion.

36.2 Disadvantages and legal drawbacks

Many legal doctrines face structural limitations in immersive environments. Contractual enforcement becomes difficult when avatars interact anonymously or when parties are pseudonymous. Jurisdictional uncertainty undermines dispute resolution when platforms operate globally without clear legal domiciles. For instance, determining applicable law under Rome I and II Regulations in cross-border avatar interactions remains unresolved.

In company law, DAOs challenge core legal assumptions, such as centralized management or shareholder liability. Without a recognized legal personality, it is unclear how to assign liability or enforce member rights. Similarly, consumer protection law struggles with novel challenges like dark patterns in immersive UI or the returnability of non-tangible goods (e.g. NFTs).

IP enforcement is also weakened by the territorial nature of copyright and trademark law, which clashes with the global, decentralized nature of virtual platforms. Legal protection for animated or AI-generated designs is not harmonized, and patent law still lacks clarity on whether metaverse-specific technical contributions (e.g. interactive simulations) are patentable.

36.3 Legal Gaps

Key legal gaps concern liability attribution, property classification, and data control. For example, virtual real estate is often licensed, not sold, but the exact legal nature of this right remains undefined in most jurisdictions. Hybrid digital goods—those combining data, services, and interactivity—defy simple contractual or ownership models.

The right of personality is insufficiently adapted to virtual avatars, raising questions about identity theft, image rights, and post-mortem digital identity. Labour law is also underdeveloped in virtual world workspaces, where spatial surveillance and boundaryless availability conflict with established worker protections.

A major legal void exists around standardised legal definitions for core virtual world elements: avatars, tokens, assets, and platform status. Without harmonised concepts, legal interoperability between jurisdictions and platforms remains elusive.

36.4 Recommendations: Legal Adaptation Through Standardisation

Legal systems should prioritize functional equivalence: adapting traditional concepts (ownership, consent, liability) to digital and decentralized contexts. Laws must recognize avatars as rights-bearing proxies, especially in areas like contract formation, identity protection, and defamation.

Standardisation must support this legal adaptation by defining shared concepts (e.g. avatar identity formats, token provenance), legal metadata (e.g. licensing terms, usage rights), and enforceable defaults (e.g. dispute resolution protocols). For company law, a model statute for DAOs should be created, outlining minimal legal personhood, liability limits, and governance safeguards.

Private international law must be updated to clarify applicable law and jurisdiction in metaverse disputes. Legal standards should guide the integration of smart contracts with formal contract law, including valid consent, remedies, and platform responsibilities.

Overall, legal certainty in virtual worlds hinges on combining substantive legal clarity with interoperable legal standards. Law must shape—not merely react to—the digital architecture of tomorrow's virtual worlds.