



Sexual Harassment in the Metaverse: Legal Challenges and the Need for Intervention

Kriti Kaushik^{1*} and Amrita Singh²

¹ Assistant Professor, School of Law, GD Goenka University, Gurugram, India

² Assistant Professor, Department of Law, Prestige Institute of Management and Research,
Indore, India

kritikaushik.8193@gmail.com

Abstract. The technological evolution has unquestionably created new frontiers, seamlessly weaving itself into the fabric of our daily lives. The same technology also offers unprecedented opportunities for criminals while posing significant difficulties for law enforcement. This dichotomy is glaringly apparent in the emerging landscape of the metaverse, especially in light of the burgeoning prevalence of sexual harassment. Reports describe incidents in which virtual groping, sexual assault, and verbal abuse are inflicted on avatars, frequently those that represent women. Despite the lack of physical contact, the psychological effect on the victims is profound, with many suffering from trauma similar to actual assaults. The distinction is further blurred by the use of haptic technology, which produces simulated bodily sensations that heighten the unpleasant experience. The primary objective of this research is to analyze the efficacy of existing criminal laws vis-à-vis sexual harassment in the metaverse, identify the specific legal challenges posed by this emerging digital environment, and explore the diverse approaches adopted by various countries in response to these modern forms of virtual harm. This shall be done by employing doctrinal and comparative legal research methods. A comprehensive review of literature reveals that most jurisdictions are ill-equipped to address the unique manifestations of virtual sexual harassment. The United States shows fragmented state-level responses, while EU law lacks harmonized definitions, and Indian law is mostly silent except for broad cybercrime provisions. Across these systems, courts face significant barriers in extending traditional sexual harassment law to avatar-based offenses, resulting in impunity for offenders and inadequate redress for victims. The lack of standardized evidentiary protocols and jurisdictional rules further inhibits effective legal action. The analysis concludes that the legal systems must adapt existing statutes, develop metaverse-specific definitions, and establish protocols for digital evidence. Without these measures, virtual environments risk becoming lawless spaces for sexual misconduct.

Keywords: Criminal laws, Haptic Technology, Sexual Misconduct, Virtual.

1 Introduction

Immersive technologies such as augmented reality (AR), virtual reality (VR), and extended reality (XR) have resulted in the conception and creation of the Metaverse, a virtual ecosystem designed to simulate social and economic interactions in the real world. What was initially conceived as a digital extension of human connectivity is now an educational, commercial, gaming, and socializing platform. However, the very factors that make the environment appealing, anonymity, realism, and interactivity, have simultaneously opened doors to unprecedented criminal activities, especially sexual misconduct [1].

The Metaverse, as immersive as it may seem, comes with a set of new challenges. With the introduction of haptic devices, which enable immersive interaction with VR platform users, harassment through voice or text becomes obsolete. This creates a fusion of virtual and physical experiences, elevating the psychological harm inflicted on victims. Recent surveys highlight alarming statistics. A study conducted by Norton LifeLock in 2022 found ¼th of women using VR platforms reported harassment or inappropriate behaviour, coupled with the Metaverse Safety Report in 2023, stating that 35% of all interactions contained unwanted groping or touching of avatars [2].

Table 1. Percentage of platform-wise women’s sexual harassment.

Source - [2]

Country/ Region	% of Female Users Reporting Harassment	Major Platform Implicated
United States	26%	Meta Horizon Worlds
European Union	22%	VRChat, AltspaceVR
India	18%	Roblox, Meta Horizon Worlds
Global Average	25%	Mixed Platforms

The idea is complex because legal systems, which claim to define violation of sexual abuse based on abuse of physical contact, virtual spaces lack physical touch contact. Numerous individuals report that they endure trauma akin to physical attack, demonstrating that the damage inflicted by psychological violence surpasses that of physical violence. Haptic feedback systems have occasionally been employed to elicit these sensations. These technologies provoke ethical and legal dilemmas about the classification of simulated violent activities with physical feedback as sexual violence under legal statutes.

The proliferation of the Metaverse in social and economic domains renders these enquiries imperative. The Metaverse industry, encompassing e-commerce, gaming, and social networking, is projected to reach USD 936 billion by 2030. The rise in virtual interactions significantly amplifies the possibility for avatar-based sexual abuse, necessitating extensive legislative responses [3].

This research focuses on the intersection of technology, law, and gender justice with the following questions -

- Why are the existing frameworks of laws and virtual sexual harassment inadequate?
- The legal frameworks for prosecution and evidence of the offense, and their absence in jurisdictions.
- The response of the United States, the European Union, and India to such matters.

This paper employs comparative and doctrinal legal research methodologies along with an analytical review of relevant legislation, jurisprudence, and academic writings. The primary aim is to devise a legally sound and practically feasible solution with appropriate mechanisms of accountability and victim protection, balancing the competing imperatives of technology and victim protection.

2 Problem Statement

Sexual harassment within the Metaverse serves as a case study capturing the juxtaposed nature of why some technological advancements are paradoxically beneficial. Unlike real-life interactions, the Metaverse enables hyper-realistic and sophisticated social interactions. Harassment in the Metaverse, unlike social media platforms where assaults are typically vocal, manifests as immersive spatial invasions or “virtual touches.” Such activities frequently target avatars, particularly those identified as female or LGBTQ+, thus reinforcing and upholding the prevailing patriarchal and gendered frameworks of society [4].

2.1 Nature and Forms of Virtual Sexual Harassment

These occurrences range from verbal abuse and unwanted sexual advances to haptic technology-based virtual sexual assault and sexual harassment simulations. Consider

the instance of “virtual groping” that was brought to light by a user of Horizon Worlds in December 2021. Shortly after entering a public space, she reported that a stranger touched her. A public debate about the misuse of safety precautions on supposedly “adult” VR platforms was sparked by this case. These incidents demonstrate how people’s use of hypermedia environments in the current world increases their vulnerability to exploitation, stemming from the avatar’s ability to make users feel physically present [5].

2.2 Psychological Impact and Legal Gaps

The application of such logic in virtual contexts appears exceedingly dubious. The psychological injury seems to manifest distinctly. Victims articulate a diverse array of emotions, primarily emphasising sensations of violation, worry, and trauma. The 2023 survey by the XR Safety Initiative revealed that 67% of participants who experienced VR harassment sought therapy for mental health disorders, including PTSD, following the incident [6].

2.3 Technological Intensification - The Impact of Haptic Devices

Beyond merely enhancing the user experience, haptic feedback technology challenges the notion of harm in the virtual realm. By capturing physical feelings, acts of aggression, and injuries experienced in the virtual realm, one can attain greater realism. This engenders delicate legal and ethical concerns on: 1) Does haptic-enabled harassment count as “physical contact” in terms of the law?, and 2) Can virtual consent be given, assumed, or be required in some cases?

Because of the law's ambiguity, perpetrators can easily escape prosecution, leaving victims with no real legal protection.

2.4 Challenges of Enforcement and Jurisdiction

Due to the inherently international nature of virtual places, attributing jurisdiction proves challenging, particularly in cases of transnational crime. Who has the jurisdiction to prosecute when both the perpetrator and the complainant live in different countries? The problem arises even when speaking about a single jurisdiction; if the offender hides behind an avatar and needs to be identified, the case becomes a complex form of digital forensics that many police departments are not equipped to solve. In addition, the platforms' operators do not take responsibility and instead cite terms of service that shift liability to ostracized users [7].

2.5 Why Current Legal Frameworks Fail

The Bharatiya Nyaya Sanhita (2023; replacing the Indian Penal Code, 1860), the IT Act, 2000, EU directives, and state-level harassment laws in the U.S. were drafted well before the advent of immersive technologies [8]. As a result, these laws -

- Only recognize sexual harassment as physical contact or as an activity limited to the workplace.

- Fail to consider avatars as embodiments of people.
- There are no standards for evidence concerning digital embodiment and simulation of the senses.

Table 2. Challenges and dimensions of offenses.

Source - [8]

Dimension	Challenge
Definition of Offense	No metaverse-specific definition of sexual harassment
Evidence	Proving avatar identity and intent
Jurisdiction	Cross-border disputes; lack of harmonized rules
Platform Accountability	Operators claim immunity under “safe harbor” provisions
Victim Redressal	No clear mechanism for complaints or compensation

3 Research Questions

The need to resolve ambiguities and contradictions within the scope of criminal law and immersive technology motivates the research. The following questions guide the research:

- What is the nature of sexual harassment in the Metaverse?
- What legal classifications can be made of avatar-interfaced abuse, which includes verbal, gesture, and haptic interactions?

- What is the scope of the current laws on sexual crime and cybercrime in immersive spaces?
- What legal solutions exist for conflicts involving cross-border perpetrators, digital personas, and the virtual evidence's acceptability?
- What legal approaches have the United States, the EU, and India taken on these issues?
- What policies can be designed to create the much-needed accountability in the Metaverse while encouraging creativity and digital freedom?

4 Purpose Of The Study

This study aims to address gaps in criminal law governing harassment in the Metaverse and to develop policies that protect users from such actions. More specifically, the objectives of the study are:

Analyze the absence of international and domestic laws about avatar-based sexual harassment.

Examine the psychological and sociological effects of immersive harassment, particularly where the use of haptic technology augments the assault.

Review the United States, the European Union, and India's respective approaches to addressing virtual crimes from a comparative perspective.

Develop specific protocols for the metaverse about definitions, jurisdictional boundaries, cross-referencing standards, and evidence processes.

The study aims to add to debates on digital rights, gender issues, and the regulation of virtual spaces and cybercrime by bridging these gaps.

5 Research Methods

This research takes a targeted approach by conducting a critical evaluation of laws, court rulings, and policy papers on sexual harassment, cyber offenses, and safety in immersive technologies and their digital counterparts. This entails engaging with specific legislation, including the BNS, 2023, IT Act, 2000, and POSH Act, 2013, as well as the comparable frameworks of the US and the EU. This study aims to examine the extent to which the legal frameworks of various jurisdictions can adapt to the Metaverse through doctrinal research [9].

The study examines how different legal systems respond to virtual sexual harassment using a comparative method in addition to doctrinal research. Interest is piqued by the US's patchwork, state-level legislative approach, the EU's emerging digital regulatory framework, and India's broad strategy centred on cybercrime laws.

This method enables examination of both the most effective policies and the most significant gaps.

The examination of primary and secondary materials helps address the research enquiries related to the notion of virtual injury. The XR Safety Initiative research and the OECD's Digital Economy Outlook offer significant insights into the extent and impact of harassment in immersive environments. These, in conjunction with scholarship in cyberlaw, feminist legal theory, and criminology, inform the discourse on the theosophical and pragmatic aspects of virtual harm and the influence of virtual environments on gendered perceptions of legal accountability [10].

The emphasized works establish the foundation for comprehending the gendered dynamics and legal ramifications of cyber damage, which are crucial to this research. Although the methodological gaps, including the lack of empirical data on offenses in the Metaverse, pose challenges to the validity and reliability of the research, the use of secondary sources ensures that the findings are well-supported and well-reasoned.

6 Literature Review

6.1 Conceptual and Legal Framework on Cyber Harassment

Bailenson (2018) asserts that virtual reality technologies can create strong senses of embodiment, enabling users to experience virtual forms of harassment as if they were real. He underscores the sociopsychological continuity that exists between real and virtual harassment, thus rendering virtual harassment important legally and morally [11].

Citron (2014) in *Hate Crimes in Cyberspace* analyzes the phenomenon of online and platform-centered gendered harassment as an amplification of harassment as a civil rights issue. Although the work predated the Metaverse's omnipresence, some of Citron's concepts, such as the disregard for vigorously enforced anonymity and a legal framework to curb harassment, are indispensable to the discussion of immersive environments [12].

Döring et al. (2022), in their article *Sexual Harassment in Virtual Reality* (published in the *Journal of Media Psychology*), discuss VR harassment and its emotional impacts. They are among the first to document how virtual reality-based harassment triggers emotions akin to real-life harassment. They also argue that the concept of digital embodiment should be considered when legally defining sexual harassment [13].

6.2 Jurisdiction and Challenges of Digital Crime

Kerr (2020) in *Cybercrime: Law and Procedure* tackles the issue of the cross-border cyber offence's jurisdictional problem and the immersive environments as an aggravating factor where acts take place in decentralized servers [14].

Koops and Goodwin (2017), in their work *CyberSpace and the State: Towards a Regulatory Model for the Internet*, examine the challenges posed by jurisdictional domains of law within the internet. This also underscores the growing necessity for comprehensive international standards to mitigate offences such as virtual sexual harassment [15].

6.3 Psychological Impact and Ethical Concerns

Fox and Tang (2017) link harassment in gaming and virtual reality (VR) environments. Their research corroborates the assertion that more immersive interaction modalities can lead to greater harm amplification, as evidenced by the Metaverse case reports [16].

Madary and Metzinger (2016) assert that ethical issues pertaining to safety and user consent in virtual reality (VR) technology must be confronted. Their ideas demonstrate a breach of the user consent paradigm, necessitating that developers be held accountable for violations of safety and consent, hence highlighting the need for more stringent standards [17].

6.4 Comparative Perspectives on Regulation

Dus (2022) offers a comparison of the UK and EU's approaches to online harassment. Mills noticed a lack of attention given to fully immersive environments such as the metaverse. He further explained that the EU Digital Services Act created certain responsibilities for the platforms, but there is no mention of offenses that occur through avatars [18].

Halder and Jaishankar (2016) explored the Indian legal frameworks in relation to the IPC and IT Act. They highlight that although there is provision for cyberstalking and obscene representation, there is no provision for immersive acts of harassment [19].

6.5 Feminist Legal Theory and Digital Gender Based Violence

MacKinnon (1989) in *Toward a Feminist Theory of the State* argues that the law tends to reflect and reinforce the existing system of male dominance. This theory can be applied to the digital realm. Although virtual harassment does not take a physical form, it does subjugate women and highlights the need for reform based on gender justice [20].

Franks (2019) in *The Cult of the Constitution* highlights the impact of technological contexts on the perpetration of gendered violence by pointing to insufficient enforcement mechanisms. She argues for constitutional protective clauses that would guard women from virtual violations and thereby preserve their autonomy and dignity [21].

6.6 Cyberlaw and Principles of Jurisdiction

Kuner (2021) in *The Internet and Jurisdiction: Adapting Legal Frameworks to a Borderless Digital Sphere* discusses the problem of applying territorial laws to activities located in decentralized spaces. His comments on the failures of enforcement in the context of the Metaverse are most relevant to sexual harassment, where the perpetrator and victim are in different legal jurisdictions [22].

Lessig (1999) in *Code and Other Laws of Cyberspace* argued, “code is law.” He was pointing to the fact that a great deal of human behavior is controlled by technology, often much more effectively than by legal statutes. This contributes to the debate about whether governance of the Metaverse by the platforms themselves would be adequate as a replacement for or addition to state regulation [23].

6.7 Cross-Jurisdictional Issues

Edwards and Harbinja (2019) analyze the controversies regarding the European Union’s Digital Single Market strategy and the shortcomings of the Digital Services Act in addressing immersive environments. They state that the focus on content moderation leaves unaddressed conduct-based harms, such as virtual sexual assault [24].

6.8 Research Gaps

Based on the reviewed literature, four main gaps have been identified :

- No agreement on the elements that constitute sexual harassment in virtual settings.
- Existing legal principles do not provide solutions for spatially boundless virtual domains.
- Inadequate standards for the admissibility of virtual evidence session recordings and haptic logs.

7 Findings & Discussion

7.1 United States

There is no comprehensive federal policy addressing immersive harassment in the Metaverse, as the US legal system addresses harassment through fragmented state laws. Workplace sexual harassment is governed by laws like Title VII of the Civil Rights Act of 1964, which does not extend to social virtual spaces. State-level laws on cyber harassment do criminalize online abuse, but only under stringent criteria such as explicit threats or obscene virtual groping, which excludes immersive gestures [25].

A notable case is *U.S. v. Drew* (259 F.R.D. 449 (C.D. Cal. 2009)) in which the court prosecuted cyberbullying that led to a minor's suicide under the Computer Fraud and Abuse Act. While this case is far from the Metaverse context, it does show that the courts are willing to interpret cybercrime laws far beyond their intended use. That said, the legal system remains untested in court cases involving immersive sexual harassment.

Contemporary discussions, including those in the American Bar Association (ABA) Cybersecurity Task Force Reports, 2022, propose updating the definitions of cyberstalking and harassment to include behaviors conducted in virtual reality environments. Meta and other virtual reality companies have implemented "Personal Boundaries" to limit the avatar proximity to one another, but these measures are voluntary, and hence, not legislated [26].

7.2 European Union

The DSA 2022, as part of the Digital Services Act, places a high emphasis on the responsibility of the platforms and the self-regulation culture they have adopted. However, the DSA puts a high emphasis on moderation and risk assessment, as well as content oversight on large online platforms. DSA does not put emphasis on avatar-based misconduct and harassment through haptics. Member states choose to enforce national criminal codes related to sex crimes, which, similar to the US, are restricted by the requirement of a breach of physical contact or violence, which makes these laws very difficult to apply in virtual settings [28].

The Council of Europe's Budapest Convention on Cybercrime, 2001, offers a skeletal structure for the prosecution of online sexual exploitation, but the limited material scope of the convention, which encompasses only child exploitation material and explicit threats, is troubling. It does not account for virtual harassment as long as there is no material or monetary damage involved [28].

7.3 India

In India, the legal approach to sexual harassment takes into consideration the following factors -

Bharatiya Nyaya Sanhita, 2023 - Outraging modesty, sexual harassment, and insulting the modesty of women are offenses under the law.

Information Technology Act, 2000 - Privacy breach by capturing or transmitting images without consent is prohibited.

POSH Act, 2013 - It covers sexual harassment of women at the workplace.

Notably, these frameworks focus on a context and a specific type of violence. For instance, BNS (2023) mandates that the use of force or assault renders avatar-based violence irrelevant. Even Section 66E of the IT Act, 2000, which is about privacy

violations, does not cover psychological virtual groping or immersive harassment [29].

Halder and Jaishankar (2016) observed that the Indian cyber laws are designed without the foresight of virtual spaces, creating a void of laws and policies. Furthermore, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, create obligations of due diligence for immersive environments, but do not address immersive spaces.

7.4 Primary Legislative Issues in Combating Virtual Sexual Harassment

Most legal scholars focus on physical contact as a form of sexual harassment. This does not apply in the Metaverse, where avatars can perform ‘groping’ and other unwanted movements that are psychologically damaging but are non-physical. Bailenson (2018) further states that the “v” in VR for virtual reality stands for a form of reality that still feels real, and that the law is still based on the physical world.

In virtual contexts, identity masking and lack of physical remnants make determining blame difficult. Within the virtual world, session logs, haptic feedback, and user VR recordings all contain digital traces of actions but are not admitted as evidence in court due to the legal requirement for evidence of a different nature. Most courts use evidence as a form of filing system, as in the Indian Evidence Act in Section 65B or the US Evidence 901; digital evidence requires physical, conventional, and mundane filing. The same notion does not apply to evidence from 3 Dimensional worlds that are layered with time, space, and actions. Because of this limitation, haptic feedback and VR recordings face evidential hurdles [30].

Virtual worlds go beyond geographic borders. If an individual from one nation tries to harm another individual from a different nation, it becomes a significant issue to know which court to approach. Some scholars indicate that traditional principles like *lex loci delicti* (law of the place the harm occurred) do not work in a digitally borderless world.

Most jurisdictions provide platforms with intermediary immunity due to provisions like Section 230 of the U.S. Communications Decency Act and Section 79 of the IT Act. These provisions in question are narrowed to the liability of user-generated content, and therefore, there exists a void where platforms are neither obligated to act to stop harassment nor liable for inaction [31].

Haptic feedback, which is intended to boost user engagement, adds a simulated physical dimension to virtual harassment. The ability for users to receive physical feedback during avatar-to-avatar interactions means the mental divide between real and virtual worlds decreases. Hence, the question becomes, is haptic-enabled misconduct subject to the same punitive measures as physical attacks?

Legal structures today do not consider the notion of sensory simulation in determining responsibility, which leaves the abused without means of compensation.

7.5 Actual Events Illustrating the Issue

A woman claimed she was virtually groped during a public session. Afterward, Meta added “Personal Boundary” features, but no legal action was taken because of definitional gaps. XR Safety Initiative documented multiple instances of coordinated harassment whereby participants used avatars to encircle other users and simulate sexual activities [32].

A complainant approached the Cyber Crime Cells with a case of VR-based threat and obscene behavior. However, the police could apply only Section 67 of the IT Act (obscenity) because there were no other targeted legal frameworks [33].

Table 3. Comparison Table regarding regulations of online platforms between the US, EU, and India.

Source - [33]

Aspect	U.S.	EU	India
Definition	No immersive-specific laws	No metaverse-specific directives	No virtual harassment definition
Platform Duty	Voluntary measures (boundary settings)	Mandatory risk assessments under DSA	Grievance redress under IT Rules
Jurisdiction	State law-driven, fragmented	Harmonized under EU framework	Territorial, limited cross-border reach

8 Conclusion

The Metaverse has the potential to redefine the way we interact with each other digitally. However, excessive sexual harassment occurring in these spaces threatens to undermine that potential. Unlike other forms of online abuse, immersive forms of harassment could be both physically and psychologically damaging due to the embodiment and haptic feedback associated with such actions.

The case study showcases the lack of legal provisions within these jurisdictions, the US, the EU, and India, given that all three lack legal frameworks to address the challenges of immersive environments. If left unchanged, the Metaverse could turn into a violent digital space where acts of gender violence and harassment are normalized and go unpunished. Legal systems need to establish specific laws for the Metaverse, create frameworks for international collaboration, and regulate the digital evidence systems and liability of the platforms. To protect users' rights, a risk-free, inclusive, and perpetual space, we need an integrated solution from the legislators, the judiciary, and the technology companies. The Metaverse can only be a place of empowerment if we can protect users from violence and establish systems of inherent responsibility.

9 A Way Forward

The legal and policy approach to mitigating sexual harassment within the Metaverse needs to be comprehensive and coherent to protect users and promote innovation simultaneously. Lastly, statutory modification is of immediate priority. For countries such as India, the US, and the EU, current legislation does not cater to avatar-based sexual harassment since the legal frameworks applicable do not accommodate a virtual form of sexual harassment based on a bodily infliction existing as one of the core prerequisites. It is the responsibility of the legislature to permit rape and sexual harassment in the form of virtual carrying out, gestures, and haptic movements using avatars within virtual spaces.

It is essential to address the gap within existing legislation that leads to the absence of legal support for victims within the nebulous environment. For example, India can merge BNS, 2023, by providing the enforcement decree, allowing the incorporation of digital embodiment, while the IT Act can be modified to include immersive interactions. The EU can work towards a Metaverse Safety Directive, and the US needs a Federal Law for the enforcement of unified legal protection.

Another major challenge is the intricacies of jurisdiction. The traditional principles, such as *lex loci delicti*, do not work for virtual borderless spaces. A victim-centric jurisdiction model is best, where the victim can pursue actions for redress in their country even if the perpetrator resides elsewhere. Globally, the Budapest Convention on Cybercrime should be modified to include immersive crimes as well as establish expedited agreements for cross-border collaboration via MLATs for coordination to be done seamlessly.

There is an immediate concern with evidentiary matters. Courts have not developed uniform methods to verify the existence of virtual reality evidence such as session recordings, avatar logs, and haptic feedback. Evidence law should be

reformed to allow for the preservation and protection of the data's authenticity, thus reinforcing its admissibility. Training judges, coupled with workforce development in digital forensics for immersive spaces, will help bolster enforcement.

Accountability of the platforms also needs to be addressed. The safe harbor provisions in Section 230 of the Communications Decency Act and Section 79 of the IT Act offer protection to the platforms and relieve them from bearing any legal consequences. These provisions can be modified to include proactive obligations such as setting up user-controlled interfaces, boundaries, and automated reporting tools on interactions. It is expected that platforms will also be obligated to conduct audits on compliance and report on the transparency of the safety measures undertaken.

References

1. M. Chawki, S. Basu, K.-S. Choi, Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety, *Laws* 13(3) (2024) 33. DOI: <https://doi.org/10.3390/laws13030033>.
2. Norton LifeLock, *Cyber Safety Insights Report: Special Release – Online Harassment in Virtual Worlds*, NortonLifeLock Inc., 2022. [Available Online: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/infographics/2022_NLCSIR_HomeFamily_Report_FINAL.pdf].
3. S. Sharma, J. Singh, A. Gupta, F. Ali, F. Khan, D. Kwak, User Safety and Security in the Metaverse: A Critical Review, *IEEE Access*, vol. 11, pp. 118723–118745, 2023. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10520714>.
4. Hine, E., Rezende, I. N., Roberts, H., Wong, D., Taddeo, M., & Floridi, L. (2024). *Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations*. *Digital Society*, 3, Article 33. Available at: <https://link.springer.com/article/10.1007/s44206-024-00114-1>.
5. Tanya Basu (2021, December 16), *The metaverse has a groping problem already*, MIT Technology Review. [Available online at: <https://archive.org/details/the-metaverse-has-a-groping-problem-already-mit-technology-review>].
6. X Reality Safety Intelligence (XRSI), *An urgent need for global regulations and governance for AI and emerging technologies: A Roundtable Report*, XRSI, San Francisco, December 2023. Available from: <https://xrsi.org/publication/an-urgent-need-for-global-regulations-and-governance-for-ai-and-emerging-technologies-a-roundtable-report>.
7. C. Bermejo Fernández, P. Hui, Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in the Metaverse, *arXiv*, 2022. arXiv:2204.01480 [cs.CY].
8. B. Gupta, A. Mangal, *Metaverse & Privacy: Navigating Legal and Security Concerns Under Data Protection Regulations*, SSRN (February 16, 2024). DOI: <http://dx.doi.org/10.2139/ssrn.4728595>
9. G. Melis, M. Monaro, Sexual Crimes in Metaverse: New Frontiers in Forensic Psychology and Legal Challenges, *Journal of Metaverse* 5(2) (2025) 124–131. DOI: <https://doi.org/10.57019/jmv.1658955>; Available at: <https://dergipark.org.tr/en/download/article-file/4695343>.
10. OECD, *OECD Digital Economy Outlook 2023*, Organisation for Economic Co-operation and Development, Paris, 2023. DOI: <https://doi.org/10.1787/c74f03de-en>.

11. J.N. Bailenson, *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do*, W.W. Norton & Company, New York, 2018.
12. D.K. Citron, *Hate Crimes in Cyberspace*, Harvard University Press, Cambridge, MA, 2014.
13. [13] N. Doring, J. Krämer, S. Mikhailova, Sexual Interaction in Digital Contexts and Its Implications for Sexual Health: A Conceptual Analysis, *Frontiers in Psychology* 34(2) (2022) 79–90. DOI: 10.3389/fpsyg.2021.769732.
14. O. Kerr, *Computer Crime Law*, West Academic Publishing, St. Paul, MN, 2021
15. Koops, B.-J., & Goodwin, M. *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law*. Tilburg Institute for Law, Technology, and Society, Tilburg Law School Research Paper No. 5/2016, December 20, 2014; DOI:10.2139/ssrn.2698263.
16. J. Fox, W.Y. Tang, Women's experiences with general and sexual harassment in online video games: Rumination, organizational responsiveness, withdrawal, and coping strategies, *New Media & Society* 19(8) (2017) 1290–1307. DOI: <https://doi.org/10.1177/1461444816635778>.
17. M. Madary, T. Metzinger, Real virtuality: A code of ethical conduct, *Frontiers in Robotics and AI* 3(3) (2016) 1–23. DOI: <https://doi.org/10.3389/frobt.2016.00003>.
18. N. Lorenzo-Dus, *Digital Grooming: Discourses of Manipulation and Cyber-Crime*, Oxford University Press, Oxford, 2022. DOI: <https://doi.org/10.1093/oso/9780190845193.001.0001>.
19. D. Halder, K. Jaishankar, *Cyber Crimes Against Women in India*, SAGE Publications, New Delhi, 2016.
20. C.A. MacKinnon, *Toward a Feminist Theory of the State*, Harvard University Press, Cambridge, MA, 1989.
21. M.A. Franks, *The Cult of the Constitution*, Stanford University Press, Stanford, CA, 2019.
22. C. Kuner, Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1), *International Journal of Law and Information Technology* 18 (2010) 176–193. Available at SSRN: <https://ssrn.com/abstract=1496847>.
23. L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.
24. L. Edwards, E. Harbinja, *Law, Policy and the Internet*, Hart Publishing, Oxford, 2019.
25. J. Webb, S. McKenzie, R. Doss, H. Zheng, R. Gorur, G. Pye, W. Yeoh, A user-centric taxonomy of cyber harm in the metaverse, *International Journal of Law, Crime and Justice* 81 (2025) 100734. DOI: <https://doi.org/10.1016/j.ijlcrj.2025.100734>.
26. American Bar Association (ABA), *Cybersecurity Tech Report 2022*, American Bar Association, Washington D.C., 2022. [Available Online: https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity/].
27. F. Di Porto, D. Foà, S. Ennis, Emerging Virtual Worlds: Implications for Policy and Regulation, CERRE Tech Media and Telecom Report, Centre on Regulation in Europe (CERRE), February 2024. Available from: https://cerre.eu/wp-content/uploads/2024/02/CERRE_Virtual_Worlds_Report.pdf.
28. C. Ryngaert, Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts, *German Law Journal* 24(S3) (2023) 537–550. DOI: <https://doi.org/10.1017/glj.2023.24>.
29. Rigotti, C., & McGlynn, C. (2025). Online and technology-facilitated violence against women: The EDVAW Platform's contribution to human rights protection and monitoring. *Netherlands Quarterly of Human Rights*. Advance online publication. DOI: <https://doi.org/10.1177/09240519251334080>.

30. M. De Fino, F. Cassano, G. Bernardini, E. Quagliarini, F. Fatiguso, On the user-based assessments of virtual reality for public safety training in urban open spaces depending on immersion levels, *Safety Science* 185 (2025) 106803. DOI: <https://doi.org/10.1016/j.ssci.2025.106803>.
31. A. Taeihagh, Governance of Generative AI, *Policy and Society* 44(1) (2025) 1–22. DOI: <https://doi.org/10.1093/polsoc/puaf001>; Available at: <https://academic.oup.com/policyandsociety/article/44/1/1/7997395>.
32. X Reality Safety Intelligence (XRSI), *An urgent need for global regulations and governance for AI and emerging technologies: A Roundtable Report*, XRSI, San Francisco, December 2023. Available from: <https://xrsi.org/publication/an-urgent-need-for-global-regulations-and-governance-for-ai-and-emerging-technologies-a-roundtable-report>.
33. TNN, SI transferred to VR over sexual harassment charges, *The Times of India*, 13 August 2025. Available from: <https://timesofindia.indiatimes.com/city/vijayawada/si-transferred-to-vr-over-sexual-harassment-charges/articleshow/123287401.cms>. pp. 135–148. DOI: https://doi.org/10.1007/978-3-540-70545-1_14

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

