INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBERCRIME IN VIRTUAL REALITY: CHALLENGES AND OPPORTUNITIES FOR INDIAN LAW ENFORCEMENT

AUTHOR - ISHA JOHNSON* & SUGANYA JEBA SAROJINI**

* LAW STUDENT (FINAL YEAR) BA.LLB SCHOOL OF LAW, CHRIST (DEEMED TO BE UNIVERSITY) LAVASA CAMPUS, PUNE

** ASSISTANT PROFESSOR, CHRIST (DEEMED TO BE UNIVERSITY) LAVASA CAMPUS, PUNE.

BEST CITATION - ISHA JOHNSON & SUGANYA JEBA SAROJINI, CYBERCRIME IN VIRTUAL REALITY: CHALLENGES AND OPPORTUNITIES FOR INDIAN LAW ENFORCEMENT, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (8) OF 2025, PG. 281-288, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

Virtual reality (VR) has transformed online interaction, establishing interactive communication, entertainment, education, and business spaces. This has created avenues for cybercrime, such as identity theft, financial crimes, online stalking, and data collection without consent. India's cyber laws, such as the Information Technology Act, 2000 and the Indian Penal Code, are ill-equipped to respond to these challenges. Law enforcement authorities are confronted with special challenges in detecting, investigating, and prosecuting crimes that occur in VR spaces because of the jurisdictional complexity of VR platforms and the challenge of obtaining digital evidence.

Virtual reality (VR) is yielding new cyber attacks, such as fraud, harassment, and cybercrime. Financial security, ethical issues, and reputational damage are threatened by these risks. The psychological effects of VR harassment and fake abuse are complicating legal intervention. The government and policymakers must reimagine cyber legislation, incorporate AI-powered security software, and introduce strong compliance policies among VR creators. Policymakers must increase digital content forensic capabilities, impose identity authentication, and enhance global cooperation to counter cross-border cybercrime. Public education campaigns, corporate accountability mechanisms, and ethical design principles must be prioritised to prevent abuse and guarantee digital security.

This Paper discusses India's legislative limitations towards combating VR cybercrime, proposes modifications, and delves into AI-based moderation, forensic software, and identification authentication. Solutions include VR-oriented cyber law, enhancing forensic expertise, and coordinating development activity with VR developers.

Keywords - *VR, Cybercrime, law, Challenges, India.*

INTRODUCTION

"*Technology is a useful servant but a dangerous master*," quoted by the renowned Christian Lous Lange, a Norwegian politician, historian, and Nobel Peace Prize winner. He delivered the quote in a speech during the 1920s, expressing concerns about how governments could misuse technology to control and oppress their citizens[316].

Virtual reality (VR) has moved from a niche idea to a fundamental aspect of contemporary digital environments, revolutionising how people engage with technology. VR is no longer

[316] Christian Lange, Nobel Lecture, NobelPrize.org (May 1, 2025), https://www.nobelprize.org/prizes/peace/1921/lange/lecture/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

limited to gaming and entertainment; it has invaded other sectors like education, healthcare, business, defence, and even social networking[317].

According to the Merriam-Webster dictionary, virtual reality is " an artificial environment which is experienced through sensory stimuli (such as sights and sounds) provided by a computer and in which one's actions partially determine what happens in the environment"[318], with the capability to mimic real-world settings and interactions, VR provides users with an experience that goes beyond conventional digital interfaces. Although this technology has brought revolutionary options, it has also brought with it unease about cybersecurity, digital identity theft, invasions of privacy, and how virtual acts have legal consequences[319].

Technology brings people together, transforming their interactions and lives in an ever-changing symbiosis. Rather than a luxury, connectivity in the digital age is now necessary, spawning new technologies, social norms, and legal challenges. For instance, the computer games industry has evolved from simple internet communication through audio and video dialogues to exciting and engaging virtual reality immersion.

Technological advancements have given rise to various legal challenges, prompting the introduction of laws and bills tailored to the digital era. One significant development is the Digital Personal Data Protection Act of 2023[320]. This statute safeguards individuals' data, focusing on consent-based processing and transfer.

The Information Technology Act of 2000[321] focuses on the legal framework of electronic commerce and electronic data interchange, and also signifies the legal aspect of digital signature and cybercrime. Cybercrime includes the legal provision of the Information Technology Act, 2000 and the Indian Penal Code, 1860[322] (replaced by new law Bharatiya Nyaya Sanhita, 2023[323]).

Technological innovations bring positive and negative impacts, making the digital era exciting and flexible. However, excessive use can lead to destructive or disruptive outcomes. Teenagers and adults, the primary technology users, may fall prey to unnoticed criminal activities. Virtual reality games exemplify advanced technology, enabling players to experience a sense of touch through digital interactions. Cybercrime legislation aims to prevent unconstitutional actions facilitated by technology. The scope of crime in digital technologies is vast and complex, involving numerous factors that exploit technology maliciously. This paper studies cybercrime and virtual reality crime while examining the legal frameworks within the Indian legal system.

As a rising digital economy, India is witnessing increasing applications of Virtual Reality (VR) and Augmented Reality (AR) across all industries. From virtual classrooms and simulated medicine to experiential financial transactions, VR has emerged as a potent technological force, while AR enriches real-world interactions with digital overlays[324]. However, as next-generation VR and AR platforms gain wider use, cybercriminals exploit such virtual and augmented spaces for criminal purposes. Cybercrime in virtual and augmented realities uniquely differs from traditional cybercrime due to virtual and augmented spaces' three-dimensional, interactive character. In contrast to conventional cybercrimes committed via text-based, audio-based, or video-based media, VR and AR crimes involve immersive experiences where people

[317] Extended Reality: The Future of Immersive Technologies, https://www.onirix.com/extended-reality/

[318] "Virtual reality." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam webster.com/dictionary/virtual%20reality.

[319] Ayah Hamad & Bochen Jia, How Virtual Reality Technology Has Changed Our Lives: An Overview of the Current and Potential Applications and Limitations, 19 International Journal of Environmental Research and Public Health 11278 (2022), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9517547/

[320] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

[321] Information Technology Act, 2000 (Act No. 21 of 2000)

[322] Indian Penal Code, 1860 (Act No. 45 of 1860).

[323] Bharatiya Nyaya Sanhita, 2023. Act No. 45 of 2023).

[324] Chourasia, S., Jodhana, L.S., Verma, B. and Shrivastava, A., 2023. Exploring the potential of augmented reality and virtual reality on Indian tourism industry. The Gurugram University Business Review, pp.40-49.

engage with digital avatars, virtual worlds, AI-driven virtual agents, and mixed reality experiences. This distinctive feature of VR and AR makes detecting, investigating, and prosecuting cyber crimes difficult, particularly in the Indian legal framework[325].

CYBERCRIME MANIFESTS IN VIRTUAL REALITY

Virtual Reality (VR) has transformed digital interactions by creating immersive virtual environments for gaming, social networking, education, and commerce[326]. This technological advancement has also brought with it unprecedented cybersecurity threats. Unlike conventional cybercrimes limited to two-dimensional spaces, VR-based offences occur in interactive three-dimensional worlds where users interact as digital avatars, participate in virtual economies, and experience simulated physical interactions[327].

This paradigm shift has created complex legal and enforcement challenges for Indian authorities. The interactive quality of VR heightens the effect of crimes - virtual groping or harassment can induce actual psychological trauma. At the same time, financial fraud in VR markets can result in appreciable monetary losses through cryptocurrency and NFT scams[328].

The Indian legal apparatus is presently not equipped to confront these new threats. The Information Technology Act, 2000[329] and the relevant Indian Penal Code sections were formulated for traditional cybercrimes and do not fully address VR-specific crimes. For example, there is no legal consideration of "virtual assault" or explicit jurisdiction over crimes committed in global VR sites. Recent cases covered by leading Indian publications highlight the loopholes - The Hindu reported on deepfake avatar scams[330] and The Economic Times brought NFT fraud cases in metaverse sites to light. The BBC report on virtual groping cases illustrates that current laws are not well-suited to such new crimes[331]. Technical shortcomings in digital forensics exacerbate such difficulties since Indian cyber cells have few means of investigating blockchain-based VR crime or tracing AI-generated deepfakes[332].

Despite these difficulties, VR cybercrime offers scope for legal and technological innovation. India can modify the IT Act[333] specifically to deal with VR offences and use the recently passed Digital Personal Data Protection Act (2023)[334] to control data collection in virtual spaces. Creating dedicated VR cybercrime branches under existing agencies such as the Indian Cyber Crime Coordination Centre (I4C)[335] would further improve investigation capabilities.

Technology-based measures like AI-driven content moderation and blockchain forensics software can be implemented to identify and prevent virtual crimes[336]. International collaboration is equally important, given that VR platforms are borderless. Public-private collaborations with VR firms may improve safety mechanisms, while campaign awareness may teach users about hazards[337]. As India becomes a runner in digital economies, anticipatory

[325] Patel, M., 2021. EMERGING TRENDS OF IMMERSIVE MEDIA IN INDIA–AUGMENTED REALITY (AR), VIRTUAL REALITY (VR) AND MIXED REALITY (MR) CASE. DR. DY PATIL B-SCHOOL, PUNE, INDIA, p.863.

[326] Virtual Reality: Exploring Boundaries and Limitless Possibilities Bar and Bench - Indian Legal news, https://www.barandbench.com/law-firms/view-point/viewpoint-virtual-reality-exploring-boundaries-limitless-possibilities

[327] Thomas, S., 2021. Investigating interactive marketing technologies-adoption of augmented/virtual reality in the Indian context. International Journal of Business Competition and Growth, 7(3), pp.214-230.

[328] Hasan, A., Nahar, K. and Akhter, S., 2024. Cryptocurrency Scams: A Multi-Pronged Approach to Mitigating Risks Through Regulation, Enforcement, and Consumer Education.

[329] Information Technology Act, 2000. (Act No. 21 of 2000).

[330] The Hindu Bureau, Most Indians have come across deepfake content online and worry about cyberbullying: Report, The Hindu, Apr. 29, 2024, https://www.thehindu.com/sci-tech/technology/most-indians-come-across-deepfake-content-online-worry-about-cyberbullying-report/article68119802.ece

[331] The Cyber Threat of Virtual Reality, BBC News (Mar. 20, 2025), https://www.bbc.com/news/technology-67865327..

[332] Sahana Venugopal & Saumya Kalia, From IT bots to AI deepfakes: The evolution of election-related misinformation in India, The Hindu, Apr. 16, 2024, https://www.thehindu.com/elections/lok-sabha/from-it-bots-to-ai-deepfakes-the-evolution-of-election-related-misinformation-in-india/article68015342.ece

[333] *Id. Act, 2000.*

[334] Digital Personal Data Protection Act, 2023.(No. 22 of 2023).

[335] National Cyber Crime Reporting Portal, Ministry of Home Affairs, https://i4c.mha.gov.in/

[336] World Economic Forum, Interoperability in the Metaverse, https://www3.weforum.org/docs/WEF_Interoperability_in_the_Met

[337] Yogesh K. Dwivedi et al., Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, 66 International Journal of Information Management 102542 (2022), https://www.sciencedirect.com/science/article/pii/S0268401222000767

action for VR cybercrime will be pivotal to safeguard users and uphold the trust in novel technologies.

Virtual reality technology has increased in importance in India. It is becoming increasingly important in gaming, education, healthcare, and socialisation. Along with these applications, legal and regulatory frameworks are now taking shape. The IT Act 2000[338] and the IPC 1860[339] can be the grounds for handling VR-related crimes. However, regulations must be drafted to solve the typical VR environment's challenges. Indian history with internet technology since 1950 has been the tale of rapid technological change and integration into the world's digital economy.[340]

India has a well-defined legal framework for cybercrime and VR crime, covered under the Information Technology Act 2000[341]. The Act elaborates on cybercrimes and the punishments, which include accessing computer systems and data, punishments for committing cyber crimes, electronic transmission of obscene material, and access. The Indian Penal Code, 1860, and the Digital Personal Data Protection Act, 2023[342] also discuss cybercrime. Virtual reality in India has also increased in usage. Such an increase has led to the usage of any platform with the features of VR and thus also to virtual harassment, robbery, and sexual offences. The current laws, such as the IT Act 2000[343] and IPC 1860[344], could not resolve these issues.

CYBERCRIME CHALLENGES IN VIRTUAL REALITY

Regulation of cybercrime in virtual reality (VR) in India has many challenges that require great attention from law enforcement and policymakers. One such significant challenge is jurisdictional complications[345]. VR websites are usually hosted by multinational corporations, leading to cross-border interfaces that make applying the law difficult. Offences conducted in VR settings can involve subjects from various countries, and fixing the jurisdiction of such crimes is a tremendous legal challenge. Indian cyber laws, like the Information Technology (IT) Act, 2000[346], mainly extend to crimes within domestic borders. Still, the absence of international treaties related to VR cybercrime renders prosecuting foreign offenders extraordinarily challenging.

A second challenge comes from the anonymity offered by VR platforms, which enables the creation of avatars that do not disclose genuine identities. Cybercriminals often use this anonymity to practice financial fraud, impersonation, and harassment. For instance, one can pose as known acquaintances or professional entities, trick other users into revealing sensitive data or participate in scam transactions. Indian legislation like Section 66 C[347] (penalises identity theft) and Section 66 D[348] (cheating by personation using a computer resource) of the IT Act, dealing with identity theft and impersonation, respectively, do not suffice to encapsulate the sophistication of avatar-based crimes in immersive VR environments.

Gathering and storing digital evidence in virtual spaces presents another major challenge for law enforcement agencies. Proof in virtual spaces usually takes the form of interaction logs, voice recordings, and digital transactions, all of which need specialised forensic equipment to extract, authenticate, and present in court. Indian agencies do not have the infrastructure and expertise to carry out such investigations efficiently, making it challenging to prosecute criminals. Furthermore, the

[338] *Id. Act, 2000.*
[339] *Id. Act, 1860.*
[340] "India - Information and Communication Technology." Trade.gov, 12 Jan. 2024, https://www.trade.gov/country-commercial-guides/india-information-and-communication-technology.
[341] *Id. Act, 2000.*
[342] Digital Personal Data Protection Act, 2023.(No. 22 of 2023).
[343] *Id. Act, 2000.*
[344] *Id. Act, 1860.*
[345] Yaman Kasturi, Cybercrime in the Digital Age: Challenges and Legal Gaps in India's Cybersecurity Landscape, African Journal of Biomedical Research 212–224 (2024), https://africanjournalofbiomedicalresearch.com/index.php/AJBR/article/view/5724/4494
[346] *Id. Act, 2000.*
[347] Information Technology Act, 2000. (Act No. 21 of 2000) s.66C
[348] Information Technology Act, 2000. (Act No. 21 of 2000) s. 66D

ephemeral nature of VR interactions means that valuable evidence can be lost if not promptly secured, adding another layer of complexity to enforcement.

A critical gap in India's legal system is the absence of explicit legal definitions for VR-specific crimes. Unlike traditional cybercrime, VR-related crimes involve unique behaviours such as virtual assault, digital harassment, and simulated financial scams. These crimes transmogrify the physical and online worlds, posing a challenge for implementing existing laws. For instance, though Section 67[349] of the IT Act precludes the circulation of obscene content, it remains silent on issues of harassment and assault that are carried out online. This grey area leaves the victims unprotected under law, so there is all the more pressure to amend existing legislation[350].

The far-reaching data-gathering activities of VR applications pose absolute privacy and ethical challenges. The applications collect user behaviour patterns, biometric information, and interaction history, which remain susceptible to unauthorised access and abuse. Cybercriminals can use these details for monetary fraud, extortion, or identity theft. Even after launching the Digital Personal Data Protection Bill [351], its ambit does not mention the specific privacy threats that VR spaces pose, making users vulnerable to surveillance and hacking.

To overcome these issues, Indian law enforcement agencies need to take a few proactive measures. The broadening of cyber laws is the need of the hour, beginning with the amendment of the IT Act to provide for VR-specific crimes. Laws dealing with crimes like virtual harassment, identity deception, and economic fraud in immersive environments must be well defined so that there is accountability. The other significant action is cooperation with technology firms. Law enforcement bodies can collaborate with VR creators to incorporate security mechanisms like AI-powered moderation, monitoring suspicious behaviour in real-time, and verifying identities to avoid impersonation and fraud.

Investment in cutting-edge digital forensic capacity is another imperative. Specific tools that trace illicit activity from within virtual spaces, like interaction tracking and avatar recognition, must be incorporated into police procedures. Officer training programs for working with VR-related evidence would also maximise investigation effectiveness. User education programs on awareness of cybercrime threats and safe practices are also necessary to inform VR users. Public campaigns may enlighten users on phishing attempts, social engineering methods, and the necessity of protecting their virtual identities[352].

Lastly, cooperation is necessary at the international level to deal with jurisdictional issues and fight transnational VR cybercrimes. The augmentation of collaboration with international cybersecurity organisations and signing bilateral or multilateral agreements can help to share information, track criminals, and conduct joint investigations[353]. By harmonising VR-related laws across borders, India can improve its response to cross-border crimes and provide justice to victims[354].

India's law enforcement apparatus is improving against VR cybercrime, which is facing particular challenges. However, these efforts need to be continuous, with continuous evaluation and adaptation to remain current with VR technology and cyber threats, and they require more research, stakeholder engagement, and policy formation.

[349] Information Technology Act, 2000. (Act No. 21 of 2000) s. 67
[350] S. Chakraborty, (2023). Virtual Reality Criminal Trials: Legal Implications and Challenges in India [Online]. 6 Issue 2 Int'l J.L. Mgmt. & Human. 1786 (2023)International Journal of Law Management & Humanities. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/ijlmhs22&div=179&id=&page=.
[351] Digital Personal Data Protection Act, 2023.(No. 22 of 2023).
[352] Shrinivaas, K.B. and Zuhayr, S., 2023. Metaverse-Legal Complications and Efficacious Remedies: An Indian Perspective. *Issue 4 Int'l JL Mgmt. & Human.*, *6*, p.2553.
[353] India and US sign MoU on Cybercrime Investigations Ministry of External Affairs, Government of India, https://mea.gov.in/press-releases.htm?dtl/38924/India_and_US_sign_MoU_on_Cybercrime_Investigations
[354] Chakraborty, S., 2023. Virtual Reality in Criminal Trials: Legal Implications and Challenges in India. *Issue 2 Int'l JL Mgmt. & Human.*, *6*, p.1786.

CONCLUSION

Virtual reality (VR) technology has grown in applications in diverse areas such as gaming, learning, healthcare, and commerce. However, it also poses cybersecurity threats that infringe upon users' security, privacy, and enforcement. These issues mandate a multi-pronged response incorporating legal reform, technological innovation, and international cooperation. The jurisdictional complexity of VR cybercrime is a significant concern, as it entails cross-border interactions between users from diverse countries. Current laws do not specifically address crimes against cyberspace, making it hard to prosecute the criminals effectively. The anonymity provided by VR sites is easy to exploit for identity theft, financial fraud, and harassment.

Indian laws such as Section 66 C and Section 66 D of the IT Act are insufficient to tackle VR-based crimes. The ephemeral nature of VR interactions makes forensic analysis more difficult, and forensic officers' specialised training programs would enhance their ability to handle VR-specific cybercrime cases. Data privacy is still a primary concern in VR, as VR applications collect vast amounts of user data, which cybercriminals can manipulate. International cooperation is also necessary to counter VR cybercrime, as most VR systems operate on global networks. Investment in AI-driven machine learning-based cyber threat detection, real-time forensic analytics, and adaptive AI-based security tools can improve cybercrime prevention.

REFERNCES:

1. Ayah Hamad & Bochen Jia, How Virtual Reality Technology Has Changed Our Lives: *An Overview of the Current and Potential Applications and Limitations,* 19 INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH 11278 (2022), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9517547/ (last visited April 1, 2024)*
2. *EXTENDED REALITY: THE FUTURE OF IMMERSIVE TECHNOLOGIES, https://www.onirix.com/extended-reality/ (last visited April1, 2024)*
3. *CRYPTOCURRENCY SCAMS: A MULTI-PRONGED APPROACH TO MITIGATING RISKS THROUGH REGULATION, ENFORCEMENT, AND CONSUMER EDUCATION, https://mpra.ub.uni-muenchen.de/121215/ (last visited April 1, 2024)*
4. *ACADEMIA.EDU - FIND RESEARCH PAPERS, TOPICS, RESEARCHERS, https://www.academia.edu/signup?a_id=68697632 (last visited April 1, 2024)*
5. *VIRTUAL REALITY: EXPLORING BOUNDARIES AND LIMITLESS POSSIBILITIES BAR AND BENCH - INDIAN LEGAL NEWS, https://www.barandbench.com/law-firms/view-point/viewpoint-virtual-reality-exploring-boundaries-limitless-possibilities (last visited April 1, 2024)*
6. *Sujo Thomas, Investigating interactive marketing technologies - adoption of augmented/virtual reality in the Indian context, 7 INTERNATIONAL JOURNAL OF BUSINESS COMPETITION AND GROWTH 214 (2021), http://www.inderscience.com/link.php?id=116266 (last visited May 1, 2025)*
7. *Sahana Venugopal & Saumya Kalia, From IT bots to AI deepfakes: The evolution of election-related misinformation in India, THE HINDU, Apr. 16, 2024, https://www.thehindu.com/elections/lok-sabha/from-it-bots-to-ai-deepfakes-the-evolution-of-election-related-misinformation-in-india/article68015342.ece*
8. Self-Sovereign Identity for Trust and Interoperability in the Metaverse, in 2022 IEEE *SMARTWORLD, UBIQUITOUS INTELLIGENCE & COMPUTING, SCALABLE COMPUTING & COMMUNICATIONS, DIGITAL TWIN, PRIVACY COMPUTING, METAVERSE, AUTONOMOUS & TRUSTED* VEHICLES

(SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta) 2468–2475, *https://ieeexplore.ieee.org/document/10189537/*

9. Yogesh K. Dwivedi et al., Metaverse beyond the hype: *Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, 66 International Journal of Information Management 102542 (2022), https://www.sciencedirect.com/science/article/pii/S0268401222000767*
10. *The Hindu Bureau, Most Indians have come across deepfake content online and worry about cyberbullying: Report, The Hindu, Apr. 29, 2024, https://www.thehindu.com/sci-tech/technology/most-indians-come-across-deepfake-content-online-worry-about-cyberbullying-report/article68119802.ece* Yaman Kasturi, Cybercrime in the Digital Age: *Challenges and Legal Gaps in India's Cybersecurity Landscape, African Journal of Biomedical Research 212–224 (2024), https://africanjournalofbiomedicalresearch.com/index.php/AJBR/article/view/5724/4494*
11. In.dia - *Information and Communication Technology*. 12 Jan. 2024, https://www.trade.gov/country-commercial-guides/india-information-and-communication-technology.
12. "Data on 40 Firms May Have Leaked in Cyberattack on JAXA Last Year | The Asahi Shimbun: Breaking News, Japan News and Analysis." *The Asahi Shimbun*, https://www.asahi.com/ajw/articles/15315931. Accessed 2 Nov. 2024.
13. Dremliuga, Roman, et al. "Crime in Virtual Reality: Discussion." *2019 International Conference on Cybersecurity (ICoCSec)*, 2019, pp. 81–85. *IEEE Xplore*, https://doi.org/10.1109/ICoCSec47621.2019.8970947.
14. Hanson, Kami, and Brett E. Shelton. "Design and Development of Virtual Reality: Analysis of Challenges Faced by Educators." *International Forum of Educational Technology & Society*, vol. 11, pp. 118–31, https://www.jstor.org/stable/10.2307/jeductechsoci.11.1.118.
15. Maamari, Victoria. "Virtual Reality Crimes: Are They Real and Can They Be Prosecuted?" *Crimlawpractitioner*, 9 Apr. 2024, https://www.crimlawpractitioner.org/post/virtual-reality-crimes-are-they-real-and-can-they-be-prosecuted.
16. Magazine, Smithsonian, and Clive Thompson. "The Walkman's Invention 40 Years Ago Launched a Cultural Revolution." *Smithsonian Magazine*, https://www.smithsonianmag.com/innovation/walkman-invention-40-years-ago-launched-cultural-revolution-180972552/. Accessed 30 Oct. 2024.
17. Sales, Nancy Jo. "A Girl Was Allegedly Raped in the Metaverse. Is This the Beginning of a Dark New Future?" *The Guardian*, 5 Jan. 2024. *The Guardian*, https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta.
18. Sarkar, Gargi, and Sandeep K. Shukla. "Reconceptualising Online Offences: A Framework for Distinguishing Cybercrime, Cyberattacks, and Cyberterrorism in the Indian Legal Context." *Journal of Economic Criminology*, vol. 4, June 2024, p. 100063. *ScienceDirect*, https://doi.org/10.1016/j.jeconc.2024.100063.
19. "THE BHARATIYA NYAYA SANHITA ." *2023*, vol. ACT NO. 45 OF 2023.

20. "Virtual Reality in Criminal Trials: Legal Implications and Challenges in India." *International Journal of Law Management & Humanities*, https://ijlmh.com/paper/virtual-reality-in-criminal-trials-legal-implications-and-challenges-in-india/. Accessed 2 Nov. 2024.