

“From Avatars to Athletes: Legal Frameworks for Addressing Crimes in Virtual Worlds.”

Mr. Subhrajit Chanda^{1*}, Dr. Deevanshu Shrivastava²

Submitted: 12/03/2024 Revised: 27/04/2024 Accepted: 04/05/2024

Abstract: This article aims on examining the legal implications that virtual crimes might have on the developing world of metaverse. It highlights on the inadequacies within the existing legal frameworks. The conventional laws frequently fall short in addressing the intricacies of virtual offenses like harassment, theft, and copyright infringement as technologies like virtual reality (VR) and augmented reality (AR) transform user interactions. The article highlights the psychological effects on victims by analysing noteworthy case studies, including instances of virtual violence. The article also acknowledges the responsibilities of the tech companies to implement a strong security or moderation systems and community guidelines to make sure that the user rights are protected. Moreover, the article also explores the different challenges that the lawmakers are facing to introduce effective legal frameworks and also offer different policy recommendations that protect users and promote safe engagement in virtual environments.

Keywords: Metaverse, Virtual Crimes, Legal frameworks, User safety, Tech Companies, Cyber Law

I. Introduction and Background

The place where people come together to create, play and try to fulfil their dreams is called the virtual world. In this world, people spend a lot of time in front of screens through ways of virtual reality and augmented reality (Yin et al., 2021). They are the two technologies that constantly changing the way people see screens and have interactive experiences. Virtual Reality is computer generated world that man experiences now and Augmented Reality is way through which individuals are transported to that virtual world though digital images and different other layers by using either visor or smartphone. Both of these realities have helped in the convergence of physical and virtual space accessed through computers and immersive technology, leading to the formation of a metaverse. Metaverse is a phenomenon which has prompted a shift in the ways in which people interact with technology in the contemporary society and also the development of the internet since people have already reached 3.0 (Mystakidis, 2022). This metaverse can create avatars which are fictional creations of imagination. This world was first termed in Hindu philosophy which means a physical manifestation of a higher being in the later world. But in the virtual world, the roles have been reversed where

the higher entity is the user and the user's digital manifestation is the avatar (Cheong, 2022).

These avatars are gaining intelligence and operating with more autonomy than humans. Again, it has been seen that blockchain technology has further developed these avatars to add more value to virtual goods. However, the rise of the metaverse brings about new challenges, notably the prevalence of virtual crimes. One of the most important threats is that virtual avatars are evolving beyond computer generated puppets to being controlled by real world users such as in virtual reality games (Barfield, 2006). These avatars have grown autonomous since they take their own decision or solve their own problems which may not be understandable to the users. Moreover, "familiar" virtual avatars, mainly controlled by users, raise various legal issues, such as using copyrighted or trademarked material and determining liability. Hence addressing these legal issues have become crucial to protect the users of metaverse. It is important to understand that metaverse can be multi-pronged since business can introduce leads in the virtual world by incorporating the customers and engaging them responsibly. Brands are now adopting group interactions in the Metaverse and digital fashion are also being offered to the users at their own price (Joy et al., 2022). But the current legal frameworks are not equipped well, to handle virtual crimes mainly sometimes because of jurisdictional issues. The recent UK case of virtual assault involved an incident within Meta's Horizon Worlds, where she described that her virtual avatar was sexually harassed after she joined the environment and felt that her rights were violated thus demonstrating how psychological impact too can prompt virtual crimes (Sales, 2024). The

¹PhD Research Scholar, School of Law, GD Goenka University, Gurugram, India. ORCID: 0000-0002-4340-9952, Email Id: suchanda811@gmail.com

²Associate Professor, Associate Dean at School of Law, School of Law, GD Goenka University, Gurugram, India. Email Id: deevanshu.shrivastava@gdgu.org

*Corresponding Author: Mr. Subhrajit Chanda,

¹PhD Research Scholar, School of Law, GD Goenka University, Gurugram, India. ORCID: 0000-0002-4340-9952, Email Id: suchanda811@gmail.com

following article thus addresses these issues comprehensively.

II. Legal Implications of Virtual Crimes

The Metaverse is a logical evolution of the internet that has been offering more immersive and authentic experiences. It is a virtual realm with a persisting environment which exists even when nobody is interacting with them. Tech companies are still clearing out on the clear definition of metaverse and hence the concept is still unclear (Carnegie UK Trust, 2022). Hence, current legal frameworks almost are not as effective to handle the complex nature of virtual crimes. There are Cyber laws developed which manage crimes that occur through internet platforms or technology related platform. It is an umbrella term since it results in two types of crime, namely cyber-dependent crime and cyber-enabled crimes. Violence by alternatives or proxies have always been in picture. There are concerns which have led to warning labels as well as content ratings even when violent images in digital media have been regularised (Sen, 2023). Meanwhile, the digital world is becoming more and more immersive. The users now are able to create virtual resources, buy assets with real money and also induce in activities like virtual art museum tours and games like Pokémon GO (McTiernan, 2024). These have resulted in many crimes of exploitation which as grooming or fraud. There are also crimes related to intimidation, deception, stalking that are an existing problem in the virtual world. It can be said that legal frameworks can be similar or identical to those in physical world. The distinctive features of virtual environments and the intricate relationships between users, virtual property, virtual currencies, and virtual world operators must be carefully taken into account when addressing legal concerns in virtual worlds (McTiernan, 2024). However, in the physical world, action which are considered as crimes, are not taken to be one in the virtual world. This is because a number of video games do allow violence and property crimes which are illegal in real life. Since players of the game do not oppose to these actions they become mutually accepted behaviours. However, this is being considered to be changed since regulations are needed even for this type of consent and prevent the user from any bullying or bigotry which current laws might now handle well. In the United States the federal and state laws that govern the virtual crimes are Computer Fraud and Abuse Act (CFAA) and Digital Millennium Copyright Act (DMCA) (Sen, 2023). In United Kingdom, Computer Misuse Act 1990 (CMA) and Investigatory powers Act 2016 (IPA) are utilized to manage these cases where as for criminal acts, it goes under Fraud Act 2006, Forgery and Counterfeiting Act 1981, Proceeds of crime act 2002 (POCA), Theft Act 1968 and 1978, etc (Sharma, 2020). However, the government of United Kingdom, did introduce a new set

of law, that is the Online Safety Act 2023 which protects children and adults online. It provides different social media companies and tech companies with duties to uphold user safety in the virtual platform. In India the legal framework of virtual crimes is Information Technology (IT) Act, 2000 (Sen, 2023).

Additionally, there are two types of virtual environment, one which is designed for only a single individual and another where many individuals participate this forming a community (Lee et al., 2021). It needs to be noted that most of the users spend a lot of time in their virtual world that in real life. Here they actively interact with other avatars. Here they are not just playing online games, they are creating a virtual world where these avatars can build a home, have new identities and even gain real wealth. In this situation an issue arises where this online role playing depends upon who owns intellectual property created in the game. Hence now the users are in needs of their basic rights even in their digital creations (Indriani & Anggraeni, 2022). But since they have non-executive, unrestricted use of their content, these rights have grown to be real life legal implications for the virtual avatars that are being created. In the case *Eros LLC v. Doe*, Eros, a Second Life adult goods manufacturer, filed a lawsuit against "Volkov Catteneo," alleging that the latter had copied and sold Eros's wares without authorization (Justia Law, 2024). Linden dollars, which are convertible into US dollars, were the price at which Eros offered these virtual goods. Eros sued in Florida under the alias "John Doe" in order to conceal their identity. They argued in the court that the leatherwood and different other unknown parties were involved in unauthorized copying. Later Volkov Catteneo admitted that they would stop copying. Hence it can be concluded that since majority of the individuals spend more time in virtual worlds, like this number of legal issues can arise which will cover legal domains of intellectual property, criminal law, contract and torts.

III. The Role of Tech Companies in Ensuring User Safety

In the contemporary society, many individuals escape into the virtual world through online games, devices and interactions. They tend to do exactly the things they do in the physical world and even better in those realities. But just because the virtual world is not real, does not mean crimes do not exist in virtual world (Maamari, 2024). The technology dates back to 1968 when virtual reality was created into the physical world (Global Data Technology, 2020). But it become more available to the customers around the year 2010. Again recently, Apple launched its virtual reality headset, thus introducing this world for the future generations (Arena et al., 2022). Nowadays virtual reality has become even more complex. Question arises as to whether crimes especially real crimes can be committed

in the virtual world. A fourth avatar captured images of the assault. In 2021, three male avatars sexually attacked Nina Jane Patel, a virtual reality user. Patel remembers feeling extremely uneasy and her body reacting physiologically. In order to share her story, the victim posted about the assault in social media. But conversely, she faced hatred and online trolling and disregard people have for virtual crimes (Sales, 2024). But in the recent events, a 16-year-old girl in United Kingdom was victim to rape in virtual reality by some adult men. This was the first case that has been taken up by the legal authorities to be investigated according to the UK laws. But as mentioned earlier, the authorities were quick to notice that it is difficult to investigate crimes in the virtual world. Hence, first, it is the responsibility of the tech companies to implement effective moderation systems to detect harmful behaviours in the virtual environments. With the usage of Content moderation in virtual reality (VR) all the user generated content can be monitored whether it follows the standards guidelines (Scheuerman et al., 2021). The content can include texts, images, videos of any actions. Because virtual reality is interactive and immersive, moderating involves not just controlling traditional content but also actions and interactions that may have an impact on the experiences of other users. It is important for maintaining a safe environment for the users and this can be done by a combination of tools. The tools are AI generated content analysis and human oversight which can preserve the integrity of the virtual experience.

Secondly, tech companies need to maintain community favourable guidelines. It is well known that the virtual spaces are filled with conversations, chats, interactions, and a lot of diverse voices. Hence, the space is messy. In order to maintain a sage online community, it is not enough to just create a space for all. It is important to set up community moderation where members can thrive in a friendly, respectable and big space (Gorwa et al., 2020). But moderation is not only about enforcing rules, but supporting a productive and positive environment. Such moderation is required to make the space inclusive and maintain the discussion in this platform to remain civil and respectful and prevent any aggressive behaviour or argument. It prevents any type of spams or trolls that disrupt conversations. Lastly it promotes quality content where the community remains focused in maintaining a high standard and exclude any type of biased or discriminated behaviour.

Thirdly, tech companies and their owners need to develop security measures to safeguard data from unauthorised access, potential breaches and misuse of content (Vojković et al., 2020). Here the companies need to make sure that they adopt encryption protocols, secure servers and induce access control with the aim of protecting the

personal information. Moreover, the companies need to implement data protection measures to maintain and store their digital assets and ensure that security an integrity is maintained.

IV. Sports Law and the Metaverse: Challenges and Opportunities

Since there is no universally accepted definition of metaverse, the technologies underpin a massive background such as the sports platform. It has been noted that the metaverse has immensely impacted the sports industry with its economic value predicted to reach \$80 billion by 2030, according to a report by Web3 Studio. Each year, it is the aim of the metaverse to engage fans from all over the world by providing them with immersive experiences such as limiting real world actions and creating new revenue streams (Demir et al., 2023). There are many top sports teams that have invested in metaverse after the success of e-sports and rise of tech enthusiasts. Virtual Stadiums and NFTs being the greatest examples. Imagine one does not have to worry about sold out tickets to see the favourite football team. Since now it can be seen from any angle within one's living room. Manchester City is developing a virtual representation of the Etihad Stadium in collaboration with Sony. Global fans can roam the stadium, interact with player avatars and other fans, and attend activities outside of regular game days with the help of a special headgear (Glebova, Gerke & Book, 2023). However, they are not the only ones that are creating virtual worlds. In the year, 2022 before the FIFA World Cup, both FIFA and Upland collaborated with each other to encourage fans and allow them to collect, then trade and at last own FIFA nft's. A virtual replica of the World Cup Lusail Stadium and a branded village with shops was available for fans to visit in Upland. Additionally, virtual training is yet another example, where metaverse have been created. In 2022, the NBA Commissioner Adam Silver introduced "Coach Nat" which was a virtual basketball coach voiced by Shaquille O'Neal (Bell, 2022). It was created with an aim to train the future NBA talent by using a VR headset. But the success of virtual sports does come with a lot of challenges.

Issues mainly arise in the domains of intellectual property, jurisdiction, tax and fintech laws. However, the legal questions that needs to be answered depends upon metaverse is centralized (managed by one company) or decentralized (managed by users). In terms of intellectual property rights, it is complicated by the extensive nature of metaverse because it is difficult to identify the creators and owners depending upon the terms mentioned in metaverse (Hassans, 2023). As demonstrated by *Hermes International v. Rothschild* (2023), when Hermes obtained damages for unapproved NFTs of its Birkin bags, trademark issues have begun. Again, when the metaverse

is decentralized, it is difficult to deduce that which jurisdiction shall tax the digital transactions. Different question arises on the areas of digital assets on the blockchains or the ways in which NFT can be classified. Currently, the law Commission of England and Wales is still reviewing the digital assets in order to bring about a solution to the jurisdictional rules (Hassans, 2023). Lastly, the metaverse can create issues in the field of fintech because it utilizes digital wallets and often uses cryptocurrencies. In the case of mostly unregulated cryptocurrency transactions, legal structures are required to safeguard consumers and handle issues with money laundering and fraud.

V. Future Directions and Policy Recommendations

From the above made analysis, it is important to note that legal systems need to be revised in order to address the particular issues posed by virtual crimes, given the rapid expansion of virtual environments and the metaverse. It has been observed that conventional laws, created to address transgressions in the physical world, frequently prove inadequate in addressing cybercrimes such as theft, violence, and harassment. Prosecution and enforcement are made more difficult by the intangible nature of these violations, jurisdictional difficulties, and anonymity. The laws need to be clear and free from ambiguities to ensure that the users are protected and provided with justice. The provisions for locating and punishing criminals, protecting virtual property, and attending to the psychological and emotional effects on victims should all be included in these frameworks. Legislators may promote safer, more reliable digital environments and the metaverse's sustainable evolution by bringing legal systems up to date with the realities of virtual interactions.

References

- [1] Arena, F., Collotta, M., Pau, G., & Termine, F. (2022). An overview of augmented reality. *Computers*, 11(2), 28. <https://www.mdpi.com/2073-431X/11/2/28/pdf>
- [2] Barfield, W. (2006). Intellectual property rights in virtual environments: considering the rights of owners, programmers and virtual avatars. *Akron L. Rev.*, 39, 649. <https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1268&context=akronlawreview>
- [3] Bell, B. (2022). Coach Nat, The NBA's Metaverse Basketball Coach, Is Both Laughable and Frustrating. <https://www.pastemagazine.com/tech/nba/nba-coach-nat-metaverse-basketball>
- [4] Carnegie UK Trust. (2022). Regulating the future: the Online Safety Bill and the metaverse <https://carnegieuktrust.org.uk/blog-posts/regulating-the-future-the-online-safety-bill-and-the-metaverse/>
- [5] Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, 3(2), 467-494. <https://link.springer.com/content/pdf/10.1365/s43439-022-00056-9.pdf>
- [6] Demir, G., Argan, M., & Dinç, H. (2023). The age beyond sports: User experience in the world of metaverse. *Journal of Metaverse*, 3(1), 19-27. <https://dergipark.org.tr/en/download/article-file/2657466>
- [7] Glebova, E., Gerke, A., & Book, R. (2023). The transformational role of technology in sports events. In *Sports management in an uncertain environment* (pp. 169-187). Singapore: Springer Nature Singapore. <https://hal.science/hal-04363588/document>
- [8] Global Data Technology. (2020). History of virtual reality: Timeline. Verdict. <https://www.verdict.co.uk/analyst-comment/history-virtual-reality-timeline/>
- [9] Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, 7(1), 2053951719897945. <https://journals.sagepub.com/doi/pdf/10.1177/2053951719897945>
- [10] Hassans. (2023). *The Metaverse and Sport: A Gibraltar Perspective*. <https://www.gibraltarlaw.com/insights/post/102il30/the-metaverse-and-sport-a-gibraltar-perspective-2/>
- [11] Indriani, M., & Anggraeni, L. B. (2022). What Augmented Reality Would Face Today? The Legal Challenges to the Protection of Intellectual Property in Virtual Space. *Media Iuris*, 5(2). <https://e-journal.unair.ac.id/MI/article/download/29339/21682>
- [12] Joy, A., Zhu, Y., Peña, C., & Brouard, M. (2022). Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens. *Strategic change*, 31(3), 337-343. https://researchportal.bath.ac.uk/files/314901442/Digital_future_of_luxury_brands_CLEAN.pdf
- [13] Justia Law. (2024). *Eros, LLC v. Doe, No. 8:2007cv01158 - Document 10 (M.D. Fla. 2007)*. <https://law.justia.com/cases/federal/district-courts/florida/flmdce/8:2007cv01158/202603/10/>
- [14] Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. arXiv preprint arXiv:2110.05352. <https://arxiv.org/pdf/2110.05352>
- [15] Maamari, V. (2024). Virtual reality crimes: Are they real and can they be prosecuted? *Crimlawpractitioner*.

<https://www.crimlawpractitioner.org/post/virtual-reality-crimes-are-they-real-and-can-they-be-prosecuted>

- [16] McTiernan, K. (2024). Ss8's Newest Lawful Intelligence Blog Is Here. Ss8. <https://www.ss8.com/crime-and-law-enforcement-in-the-metaverse/#:~:text=Many%20crimes%20of%20exploitation%2C%20such>
- [17] Mystakidis, S. (2022). Metaverse. *Encyclopaedia*, 2(1), 486-497. <https://www.mdpi.com/2673-8392/2/1/31/pdf>
- [18] Sales, N. J. (2024). A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future? The Guardian. <https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta>
- [19] Scheuerman, M. K., Jiang, J. A., Fiesler, C., & Brubaker, J. R. (2021). A framework of severity for harmful content online. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1-33. <https://dl.acm.org/doi/pdf/10.1145/3479512>
- [20] Sen, A. (2023). *Criminal Law and Virtual Reality: Exploring the Legal Challenges of Virtual Crimes and Virtual World*. Wwww.legalbites.in. <https://www.legalbites.in/topics/articles/criminal-law-and-virtual-reality-exploring-the-legal-challenges-of-virtual-crimes-and-virtual-world-932970#:~:text=1>.
- [21] Sharma, R. (2020). Legislation Related to Cyber Crimes in United Kingdom. https://www.researchgate.net/profile/Rahul-Sharma-205/publication/347439774_Legislation_Related_to_Cyber_Crimes_in_United_Kingdom/links/5fdbb9cc45851553a0c6ec2b/Legislation-Related-to-Cyber-Crimes-in-United-Kingdom.pdf
- [22] Vojković, G., Milenković, M., & Katulić, T. (2020). Iot and smart home data breach risks from the perspective of data protection and information security law. *Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy*, 11(3), 167-185. <https://hrcak.srce.hr/ojs/index.php/bsr/article/download/12916/6453/>
- [23] Yin, K., He, Z., Xiong, J., Zou, J., Li, K., & Wu, S. T. (2021). Virtual reality and augmented reality displays: advances and future perspectives. *Journal of Physics: Photonics*, 3(2), 022010. <https://iopscience.iop.org/article/10.1088/2515-7647/abf02e/pdf>