INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 1 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-1-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

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

VOLUME 4 AND ISSUE 1 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

METAVERSE: MAPPING THE LEGAL AND REGULATORY VACUUM IN THE VIRTUAL DOMAIN

AUTHOR - ANJALI BUSAR, STUDENT AT RAJIV GANDHI NATIONAL UNIVERSITY OF LAW, PATIALA

BEST CITATION – ANJALI BUSAR, METAVERSE: MAPPING THE LEGAL AND REGULATORY VACUUM IN THE VIRTUAL DOMAIN, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (1) OF 2024, PG. 283-290, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

For generations, technologists have dreamed of an era where our virtual lives become equally important as our physical realities. The 'metaverse' has the potential to be seen as the peak of evolutionary technological development that humankind can achieve in the foreseeable future. However, Metaverse is a pandora's box. Numerous issues will grow and sustain like uncontrolled information accumulation that infringes on our confidential information, prolonged harassment and threats, widespread security inadequacies, biased intelligence mechanisms, and problems with the physical and psychic well-being of an individual. A radical and sophisticated approach should be undertaken to either develop fresh legislation concerning domestic and international legal rules or analyze the present wrongdoings and fit them into the current legal architecture. Additionally, installing a separate system of checks and balances in terms of regulatory protocols such as multi-factor authentication, regulation by analogy, ESP mechanism, Penetration testing tactic, etc. in order to control the ungoverned and rampant mischievous activities in the metaverse would be the most fitting solution. The author makes an attempt to uncover prevailing obstacles, provides present laws as a basis to efficiently understand and resolve the nuances, and explores diverse remedies including suggestions of certain security practices to utilize the metaverse resourcefully.

Keywords: *Metaverse, Harassment, Injuries, Regulation by Analogy, Regulatory Protocols.*

METAVERSE BASICS- A PRIMER

The term 'metaverse' was coined in Neal Stephenson's 1992 science fiction novel 'Snow Crash', where humans, as programmable avatars, interact with each other and software agents, in a three-dimensional virtual space that uses the metaphor of the real world. Stephenson used the term to describe a virtual reality-based successor to the internet.[583]

The fusion of two Greek words namely 'meta' (beyond) and 'verse' (universe) which meant a 'world beyond the universe' led to the origin of the term 'Metaverse'. It created a virtual world with virtual reality to merge with our tangible reality. Delivering a deeply engaging experience of every possible thing that is nearly identical to the real world was the fundamental responsibility, besides being the basic premise behind this unconventional technology.

The onset of a virtual domain can be retraced to the time when our predecessors used to communicate the story through animal impersonation, painting on the walls and canvasses, the incarnation of deities, or observing traditional rituals, etc. Nonetheless, technological maturation is unfurling at a quicker rate than we can imagine. It was only yesterday when technology was equivalent to sending text messages and videos to our relatives and friends. At this moment, the world is a splendid concoction of scientific fiction and concrete existence.

[583] Mark Grimshaw, The Oxford Handbook of Virtuality (New York Oxford University Press 2014) 702

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

VOLUME 4 AND ISSUE 1 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

The metaverse is a world where virtual reality and a digital second life converge into one with a focus on social connection. For generations, technologists have dreamed of an era where our virtual lives become equally important as our physical realities. In the theoretical sphere, we would engage in interacting with our friends and colleagues in the virtual domain, we would spend money there as well on acquiring garments, outfits, and objects for our digital avatars.[584]

The metaverse has the potential to be seen as the peak of evolutionary technological development which humankind can achieve in the foreseeable future. Immersive, haptic technologies can make the experiences more daunting. The panoramic view, audio, and even touch simulation provided by the VR headsets and handheld controls create a multisensory experience, blurring the separation between the virtual and the physical.[585] However, when human interaction can take place so effortlessly, it can only aggravate the possibility of humans violating each other's rights. And therefore, such an invention requires robust legislation to ensure that the space is user-friendly and safe.[586]

Technically speaking, a metaverse is a virtual shared space with others, created by the convergence of virtually enhanced physical and digital reality. To put it simply, think of a metaverse as the next iteration of the internet, which started as individual bulletin boards and independent online destinations. Consequently, these final places will become sites in a virtual shared space — similar to how a metaverse will develop.

The working of the metaverse is identical to the real world as there are inventors, producers, sellers, and consumers. The audience/players/consumers can buy or sell whatsoever the synthetic universe has to offer. The payment method, by all means, is digital. Electronic payment systems, like credit and debit cards, load user accounts with game currencies. Alternatively, on certain platforms, users may create their own type of currency.

Numerous issues will grow and sustain in the metaverse, like uncontrolled information accumulation that infringes on our private and sensitive information, prolonged harassment and threats, widespread safeguard deficiencies, biased intelligent mechanisms, proliferating robots, and phishing senders, and diverse social issues, broadening the scope of inequalities, and problems with physical and psychic well-being.[587]

As this intertwined multiverse has started spreading its roots in every domain, it has opened gates to increased threats and adversities. As per the Center for Countering Digital Hate, about every seven minutes, a violation occurs in the popular virtual reality game VR Chat in the metaverse.[588] A report published by Citibank in March 2020 detected that the economy of the metaverse could be estimated to be a total of thirteen trillion dollars by the year 2030.

Various prediction reports anticipate that in 2023, there will be an emergence of 'metaverse winter'. Tech conglomerates will uphold investment commitments, but fewer start-up funding efforts and deals in the space would blanket the metaverse. The year will not result in significant returns instead, it will present a prospect for underlying technologies, like AR and VR, to mature.

The corporations and enterprises have started implementing the metaverse uses in multiple organisations, however, the development of the

[584] Chen BX, 'What's All the Hype about the Metaverse?' (*The New York Times*, 18 January 2022) <https://www.nytimes.com/2022/01/18/technology/personaltech/metaverse-gaming-definition.html> accessed 26 August 2023

[585] Le T, 'Sexual Assault in the Metaverse Is Part of a Bigger Problem beyond Technology' (*Monash Lens*, August 2022) <https://lens.monash.edu/@politics-society/2022/07/22/1384871/sexual-assault-in-the-metaverse-theres-nothing-virtual-about-it> accessed 16 August 2023

[586] Hithaishi Murthy, Hohfeld's Analysis of Rights and Rights in Metaverse' (2022) 4 Indian JL & Legal Rsch 1

[587] Prachi Singh & Dev Karan Rajput, 'Metaverse: Surging Need for Competent Laws with Increasing Metaverse Crimes' (2022) 5 Int'l JL Mgmt & Human 712

[588] Ganguly D and Biswas S, 'The Metaverse of Harassment and Hate - Times of India' (*The Times of India*) <https://timesofindia.indiatimes.com/life-style/spotlight/the-metaverse-of-harassment-and-hate/articleshow/92897196.cms> accessed 24 August 2023

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

VOLUME 4 AND ISSUE 1 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

technology will be influenced by standards such as transparency on the return of investment, technological advancement, and employee readiness. More than 120 billion dollars have been invested in metaverse and its related mergers and acquisitions were already announced in the first half of 2022, according to NASSCOM.

There have been different notions regarding this technology by every individual, regardless of age, but one aspect remains constant, which is that this virtual world is an amalgamation of digital life and real life. Both individuals and corporations have been planning to make the most out of this newly emerged virtual set up.

It is anticipated that the Metaverse will swap traditional internet mechanisms and become the core of personal interactions and business transactions, and hence, become the source of the most valuable user data. Metaverse opens up a world of endless opportunities for businesses to create experiences, participate in world-building, and connect with customers in entirely new ways. However, this technique is not without risks. Deepfakes, big data, and cyber-attacks are all potential threats to a brand and customer reputation. Since these sorts of technologies are already gaining traction, marketers must be metaverse-savvy.[589]

METAVERSE AND ITS MULTIFACETED CONCERNS

The comprehensive reach of the metaverse will bring several aspects of Copyright law, Criminal law, Tort law, Contract law, Data Protection law, and others into the broader picture. As every plausible break presents itself with a deficiency, the question is as the metaverse encompasses various variables such as avatars owners, creators, developers, etc, who will be responsible for what? And what adjudicatory mechanism could be used to iron out the disputes that may arise on account of the virtual interface. Ergo, the conundrum is to diagnose where the metaverse and the real world will coincide.

As the post-millennial generation platforms are plagued by assorted varieties of criminal wrongdoings, let us explore and understand some of them-

- **VIRTUAL HARASSMENT-**

Imagine an avatar getting close to you, touching or groping you without your consent in the virtual domain. This is not similar to the real-world situation wherein the victim has countless remedies for such horrific encounters. There exist boundless possibilities for such incidents to be more sneaky and impactful since the naturalism that partners with VR experiences swiftly conveys the fright experienced emotionally, psychically, and physically.[590]

The question arises whether this amounts to an assault or not, if yes, what are the countermeasures? Are there any laws that will protect the interest of the victim? Is there any official body where the incident can be reported? What punishment will be granted to the perpetrator and other numerous quandaries?

According to a report published, a woman aged 21 years reported an instance of being 'virtually gang raped' by numerous avatars, within 60 seconds of entering the metaverse. Three male avatars touched her inappropriately and took screenshots of both upper and lower body. Major platforms do offer different modes to report such incidents, such as Horizon World, after the above-mentioned incident, instituted a new safety tool called the 'Safety Zone' which created a virtual boundary around the avatar, restricting the movement of another within a set distance.

Abuse of technology has existed for as long as we can remember. However, as technology becomes ubiquitous and increasingly immersive, episodes of abuse and harassment have become widespread. People might feel

[589] Hackl C, 'Now Is the Time to Talk about Ethics and Privacy in the Metaverse' (*Forbes*, 12 October 2022) <https://www.forbes.com/sites/cathyhackl/2020/08/02/now-is-the-time-to-talk-about-ethics--privacy-in-the-metaverse/?sh=cd57395ae6cf> accessed 26 August 2023

[590] 'The Perspective Matters! Multisensory Integration in Egocentric Reference Frames Determines Full-Body Ownership' <https://doi.org/10.3389/fpsyg.2011.00035> accessed 22 August 2023

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

emboldened to display indecent behaviour when they will not face consequences for their undertakings. Such unseemly actions may also be manipulated by the strongly anchored toxic culture revolving around online gaming and social media in general.[591]

With the changing dynamics of our life, and amplified utilization of the Internet, these issues have started to see light of the day. An appalling episode like this in the multiverse leaves a perpetual cognitive impact on the injured subject, which is not different to the act done in the real world. As these instances are happening in the virtual world, what law would apply is uncertain. This blurriness enables users to act courageously without the fear of repercussions. Simply, a ban from the platform is meaningless. The IT-based solutions are inadequate, certain moderations in tech-driven systems alongside the legal framework are crucial to curb the menace.

- **PERSONAL INJURIES-**

One of the extensively played augmented reality games known as '***Pokemon Go***' requires the player to trap creatures called '***Pokemon***'. The object is to collect the maximum, for which the player has to either walk, ride a bike, or drive a car in the neighbourhood. Despite the game's overwhelming popularity, researchers claim that this yielded $7.3 billion in damage across the United States, 148 days after it set in motion, as this smart device game app has caused car accidents, injuries, and even deaths.[592]

Bearing similarity with this, the metaverse is capable enough to cause substantial physical damage analogous to the real world. As it requires the user to get equipped with head gears, to experience the world of reality away from reality, the psychological effect of this makes them completely unaware of the surroundings, triggering falling from the staircase, slipping over an obstruction, etc.

There have been reports disclosing that the metaverse is so awfully realistic and frightening that 30% of participants could not make it across a room with a simulated tightrope walk between the Twin Towers, so this could result in cardiovascular incidents.[593] Additionally, metaverse may affect the cognitive functioning of the person, as they may unknowingly approach zones with flashing lights and/or imagery that may cause discomfort or flicker-induced seizures, and even emotional injuries, as exposure to disturbing visuals may traumatize users and ultimately result in post-traumatic stress disorder.[594]

- **ENTERTAINMENT-**

Recently, Pooja Entertainment purchased virtual land in the metaverse and named it '*Poojaverse*' to announce the release of 'Bade Miyan Chote Miyan' which is going to be the first Hindi film to be released in the metaverse domain. This exceptional move is an indication of how cinematic creators are capitalizing on maturing techno mediums and markets, to boost spectatorship of their content.[595]

Additionally, virtual concerts are already in motion. In 2019, DJ Marshmello created a buzz by hosting a live gig in the game 'Fortnite' which had over 10 million viewers. Later, superstars like Travis Scott and Ariana Grande also followed the trail by having their digital avatars created. Though the metaverse has modernized the entertainment industry, many digital issues with respect to 'personality rights' have sprung up. After the termination of the contract before or at the intended date, who has the authority/copyright over the avatars of these A-listers has become a foremost concern.

[591] Wiederhold. BK, 'Sexual Harassment in the Metaverse' 479
[592] News S, 'Death by Pokemon Go? Game Caused up to $7.3bn Damage, Claim Researchers' (Sky News, 27 November 2017) <https://news.sky.com/story/death-by-pokemon-go-game-caused-up-to-7-3bn-damage-claim-researchers-11146310> accessed 18 August 2023
[593] Moore S, 'Law in the Metaverse' (*Forbes*, 23 December 2021) <https://www.forbes.com/sites/schuylermoore/2021/12/22/law-in-the-metaverse/?sh=5e67cabf45d1> accessed 18 August 2023
[594] Schwirn M, 'A Legal Minefield Called the Metaverse: Computer Weekly' (*ComputerWeekly.com*, 11 January 2022) <https://www.computerweekly.com/feature/A-legal-minefield-called-the-metaverse> accessed 20 August 2023
[595] Shah K, 'Copyright in the Metaverse - Copyright - India' (*Copyright In The Metaverse - Copyright - India*, 11 October 2022) <https://www.mondaq.com/india/copyright/1239234/copyright-in-the-metaverse> accessed 21 August 2023

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

VOLUME 4 AND ISSUE 1 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

- **COPYRIGHT INFRINGEMENT**-

Copyright laws provide safeguards to the original works of the creators/authors and grant them exclusive rights regarding the same. The metaverse poses individual setbacks in detecting copyright infringements along with the persons accountable for them. Typical search functions may not be as valuable as they are on the internet and may fail to identify infringing code contained within a blockchain.[596] The problem of not being able to identify the copyright infringers, extent, and manner of violation in the parallel world seems like a nightmare for the owners.

- **BREACH OF DATA-**

Unlike other online networking platforms, AR/VR technologies in metaverse retrieve body language, facial gestures, physical movement, and biometric data, this could be collected and compromised at a larger level. The amount of data collected can be misused by unregistered organizations gravely. Users themselves cannot manage the data with efficiency, which raises deep concerns as to who will manage the confidential particulars skillfully. The entanglements in the metaverse encompass questions related to identity theft, breach, regulation of data, data transfer, etc., which require convenient legal measures in effect.

EXISITNG REGULATIONS FOR THE WIN- BUT ARE THEY ADEQUATE?

In India, there are diverse sources which compels the need to safeguard sensitive personal information of an internet user. These include DPDP Act 2023, SPDI Rules 2011, CERT-in rules 2013, Consumer Protection E-Commerce Rules 2020, and other rules made by the Reserve Bank of India, Telecom Regulatory Authority of India, Security and Exchange Board of India, etc.

The dominant goal of the Information Technology Act (IT Act), 2000 is to preserve data integrity in cyberspace. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (***hereinafter, "The SPDI Rules"***) were enacted by the Central Government to confirm the provisions referenced under the IT Act.

The ***SPDI rules*** apply to all body corporates in India and also outside when they have an electronic system located in India. Such body corporates while collecting, receiving, or handling sensitive personal information have to issue a statement expressing clearly the information collected, its purpose, policy on disclosure, reasonable security measures adopted, and statement of policies. Further, it is mandated to secure the consent of the information provider. Negligence of the organization in data management is penalized with imprisonment, fines,[597] and payment of damages[598].

A recent milestone in the field of Data protection has been marked by the enactment of the ***Digital Personal Data Protection (DPDP) Act, 2023***. The act authoritatively dictates the role expectations of a 'Data Fiduciary'. Sincere attempts to ensure the credibility of data, institute reasonable data protection safeguards, and notify the Data Protection Board in case of any violation are the central responsibilities of a Data Fiduciary. The Data Protection Board of India will be responsible for levying substantial penalties, supervising data fiduciaries concerning data breaches, and redressing the grievances of cyber victims.

Though the DPDP Act will prosperously reshape the technology legislation in India, however, it is not devoid of errors. The law does not regulate the threats circumscribing the processing of personal data. These threats, commonly referred to as 'harm' potentially comprise loss of prestige, identity impersonation, discrimination, and unreasonable surveillance and profiling. ***Right to be forgotten*** (Individual right to restrict

[596] Jake Palmer 'Copyright in the Metaverse' (*Bristows*, 8 December 2022) <https://www.bristows.com/news/copyright-in-the metaverse/?utm_source=passle&utm_medium=post6&utm_campaign=metaversearticles> accessed 24 August 2023

[597] Information Technology Act 2000, s 72A

[598] Information Technology Amendment Act 2008, s 43A

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

VOLUME 4 AND ISSUE 1 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

the disclosure of their personal information) and ***Right to data portability*** (Taking data from the fiduciary for their personal use) as included in 2018 and 2019 Draft Bill, are omitted from the Act.

INTERNATIONAL SOLUTIONS: METAVERSE PRIVACY FRAMEWORK

The motive behind the enactment of European Union's ***General Data Protection Regulation*** (GDPR) was to safeguard the right to personal data protection while ensuring that the data travels freely within the EU. GDPR-regulated companies cannot legally process the data of the user without getting express content from the same. Article 13 required that the data collectors inform the data subject how, why, and where their personal data would be collected and used. The regulations subsequently gave the data subject an absolute right to request details from controllers as to what data is being processed. Right to be Forgotten, Rectification, Portability, Access, Object, etc are certain principles that lie at the heart of GDPR unlike the DPDP Act 2023 of India.

The GDPR is currently lacking the required resources to protect user activities in the metaverse. Therefore, modifications regarding consent, technology, data processing, and cross-jurisdictional disputes are critical before the metaverse enlarges its realm any further. The General Data Protection Regulation aimed to simplify the process for multinational companies, hoping that the less complicated the law is, the more control citizens can exercise over their data.[599]

No wonder the current national and international legal framework is a watershed moment in the field of data protection and it has made noteworthy transformations concerning cross border data transfer. However, a mechanism to resolve cross border jurisdictional issue still remains a muddled territory. **Cross-border disputes are an uphill battle in the physical world, hence ascertaining which rules would take supremacy and which courts can exercise jurisdictional powers necessitates a navigation of countless international conventions and obscure national statutes.**

VIRTUAL DATA PROTECTION LAW: "REGULATION BY ANALOGY"

The significance of privacy in the synthetic world is unquestionable. Due to the invention of virtual identity, the need for a virtual right to privacy becomes undisputed. Over the Internet, the identity of the user is unknown which grants them the privilege to convey and explore freely without any constraints. A message can be sent by a Male, Trans, Female, Minor child, White, Black, American, Asian, Chinese, Prime Minister, or even an office clerk. Even when the sender acknowledges his/her identity, there exists no way to find whether it's real or fictitious.[600]

Participating users are free to present themselves as liberated from several religious, social, economic, gendered, and financial biases. They are empowered to communicate multiple insights on sensational issues that might be reasonably challenging in the real world. However, the privacy of an individual avatar can be breached by another avatar or by the supervisor who manages and controls all the information stored and diffused on the platform or by the Government including its essential bodies.

It is pertinent to emphasize that the application of present laws concerning data privacy is substandard. The cyber frontier has risen above the concept of borders, states, and nations. As cyberspace is devoid of chartered territory, persons from any nation/state/district with appropriate technological equipment and digital connectivity can browse the web and engage in interpersonal and e-commerce transactions.

[599] Martin Baily, 'Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse' (2022) 36 Harvard Journal of Law & Technology 235

[600] Thomas C Anderson, 'The body and communities in cyberspace: A Mmarcellian analysis' [2000] 2(3) Ethics and Information Technology <https://doi.org/10.1023/A:1010001504963> accessed 16 August 2023

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

VOLUME 4 AND ISSUE 1 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

Let's understand the above situation with the help of an example, the right to privacy of an Indian citizen can be breached by an American player residing in Australia in a game hosted in Egypt and regulated by another country altogether. It will be difficult to identify where the rights are to be enforced and against whom in a case of severe infringement of privacy. This leaves the victim unguarded. Employing the real right to privacy in its natural form is undesirable.

Persistent and focused efforts can be made to create a virtual juridical framework acting as a separate system regulating the virtual world. This is known as '***Regulation by Analogy***' a model of regulation in which fundamental provisions of the real-world legal arrangement are transplanted in a virtual legal construct.[601] Acknowledging the 'virtual community' and 'virtual body' as sovereign and granting privacy can give way to an advanced principle of citizenship in the virtual domain.[602] The virtual prerogatives and obligations solicit a virtual state, which incorporates a legislature, an executive and a juridical branch. This forms the genesis of 'Digital Democracy'.[603]

COMPLEMENTARY REGULATORY PROTOCOLS RECOMMENDATIONS

As cyber universe has become more complex and cultured, the archaic surveillance systems have become redundant for contemporary attacks. Hence, the '***Two Factor Authentication***' (2FA) popularly referred to as '***Dual Factor Authentication***' can be deployed as a digital security protocol that plainly adds another skin to the original layer of protection. In simple terms, it requires providing a password first, and then another layer comprising usually a security token or biometric feature. Therefore, in a scenario where the user's password is hacked, it is not sufficient in isolation to pass the authentication check.

This 2FA technology could also take the form of **SMS-based 2FA** and **Voice-based 2FA**. After configuring the password and username, the website sends over a non-reusable verification code (one-time password-OTP), and the user should enter the same before it expires within minutes. Likewise, Voice based 2FA, contacting a user and delivering the code over a telephonic conversation. In a similar fashion, ***Multi-factor authentication, Biometric authentication, Token-based authentication, and cryptographic authentication*** have also entered the market focusing on bolstering additional security measures for the users engaged in metaverse activities.

Recently, a pumped-up unit of researchers at VIT-AP University in India created '***MetaSecure***' a passwordless authentication system exclusively for the metaverse. The aim is to secure comprehensive data efficiently. The system comprises three different techniques namely device attestation, facial recognition, and physical security keys. To login as an avatar in the metaverse, three security clearances have to be made such as facial identification, security key, and device verification.[604]

Further, ***Penetration Testing or Pen Testing***, is another technique to protect the computer system. It is an exercise conducted by a cyber security expert to identify and exploit deficiencies in a computer system. The weak spots of the tech setup are identified before the hacker can capitalize on it. Such contractors or experts are referred to as ***Ethical Hackers***.

Unbelievable true to life avatars being created by Facebook could allow users to maintain anonymity or enable children impersonate adults. Sophisticated age verification protocols and strategies to deter children from providing their personal data are mandatory to ensure data protection conformity in the metaverse.

[601] Julian Dibbell, 'A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society' (1994) 1994 Ann Surv Am L 471

[602] Paul toscano, 'Toward an Architecture of Privacy for the Virtual World' [2000] 19(1) UIC John Marshall Journal of Information Technology & Privacy Law 167-168

[603] Bart Van der sloot, 'Virtual identity and virtual privacy: Towards a concept of regulation by analogy' [2011] 2011(1) EGov Präsenz 41-43

[604] Sethuraman SC and others, 'MetaSecure: A Passwordless Authentication for the Metaverse' (*arXiv.org*, 4 January 2023) <https://arxiv.org/abs/2301.01770> accessed 15 August 2023

The ***Encapsulating Security Payload*** ("ESP") is an integral element of Internet Protocol Security for securing communications made over the Internet. It is used to encode data for confidentiality. This means that unauthorized users cannot retrieve information unless they possess decryption codes.

As we are rapidly progressing towards an integrated universe, there is a pressing need for stringent regulations and an official body responsible for enforcing the same. Lack of adequate sheltering has and surely will compromise with the sensitive information. The utilization of existing laws to tackle the current queries and insecurities relating to the metaverse is incomplete and therefore, unsatisfactory. The ever-evolving metaverse sparks interrogations that are beyond the scope of the contemporary legal framework.

In order to assess countless predicaments within the Metaverse domain demands a sustainable, cooperative, multidisciplinary approach that strikes a balance between novelty, protection, and development. The lack of regulations and the absence of a regulator in the metaverse has prompted frequent perpetrators to create fake identities and steal confidential information of the user for their advantage. The notion of user control, transparency, and fact-based decision-making should be embedded in metaverse infrastructure.

Additionally, a radical and sophisticated approach should be undertaken to either develop fresh legislation of domestic legal rules, international laws, and conventions, or crimes in the metaverse will have to be deeply analyzed in order to apply the current framework. Installing a separate system of checks and balances to control the ungoverned and rampant mischievous activities in the metaverse would be the most fitting solution.

CONCLUSION

The virtual world delivers a 360-degree experience, though it is an augmented reality, still, everything feels real. Whatever is not reality feels utterly convincing and unbelievably authentic. We have to staunchly accept that this unfolding virtual domain is exactly what our future looks like. We cannot run away from technological advancement as it embodies the development of the entire human race.

Undoubtedly, the metaverse will radically restructure the human-technology interface, but this will come at the sacrifice of grave human rights violations until regulated. The metaverse triggers various risks and complexities, that surely require significant changes in rules and regulations. The legislature is still oblivious to the notion of digital identity or avatars, NFTs, digital property, etc, making it incredibly more challenging to devise a legal architecture.

A private, extra-territorial legal framework controlled and managed by an unprejudiced and responsible body that would act as a surrogate of the government and work within the basic principles of the rule of law by adopting fair information directives, protocols, guidelines, policies, and practices, while crafting a robust methodology and legal framework to ensure the security and privacy of the global cyberspace community is an ideal method to deal with myriad inconsistencies wrapped inside metaverse.