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

VOLUME 6 AND ISSUE 3 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

VIRTUAL VIOLENCE VS REAL HARM: LEGALLY RECOGNISING VR HARASSMENT AS HUMAN RIGHTS ABUSE

AUTHOR – MR. SUJITH KUMAR, STUDENT AT SCHOOL OF EXCELLENCE IN LAW, THE TAMIL NADU DR AMBEDKAR LAW UNIVERSITY.

BEST CITATION – MR. SUJITH KUMAR, VIRTUAL VIOLENCE VS REAL HARM: LEGALLY RECOGNISING VR HARASSMENT AS HUMAN RIGHTS ABUSE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 225-233, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The advent of the Metaverse represents a seismic shift in human interaction, moving from 2D screens to immersive, embodied 3D environments. While this technological leap promises unprecedented connectivity, it has also birthed a new paradigm of violation: virtual assault. Recent incidents of "virtual rape" and aggravated harassment in social VR platforms like *Horizon Worlds* have exposed a critical lag in global legal frameworks. Current jurisprudence largely tethers criminal liability to physical contact, leaving victims of haptic and psychological violence in a legal vacuum. This paper argues that VR harassment is not merely a moderation issue but a substantive human right abuse, violating the right to security of person and digital bodily integrity. By analyzing the psychological phenomenon of "embodiment" the limitations of current statutes (including the US Communications Decency Act, the UK Online Safety Bill, and the Indian IT Act), and the trajectory of international human rights law, this paper proposes a "Human Rights 2.0" framework. We contend that the law must evolve to recognize that in a hyper-realistic digital regime, the distinction between "virtual" violence and "real" harm is a fallacy, requiring a new class of "digital personhood" rights to protect human dignity in the Metaverse.

I. Introduction: The Corporeal Crisis in a Digital Regime

The internet is no longer something we look at; it is something we inhabit. The transition from the "Internet of Information" to the "Internet of Experiences"—commonly recognized as the Metaverse—has fundamentally altered the ontology of digital interaction. In the Web 2.0 era, harassment was textual or pictorial; it was something seen on a screen, distinct from the viewer. In the Web 3.0 era, harassment is spatial, somatic, and visceral. It is an act that happens *to* the user, not just in front of them.

As technology corporations race to build immersive social VR platforms, a dark underbelly of human behavior has migrated with them. Reports of sexual assault, groping, stalking, and "virtual gang rape" have proliferated in spaces like Meta's *Horizon Worlds*, *VRChat*, and *Quiivr*. In these environments, users do not merely control an avatar; they *become* the avatar. Through the use of stereoscopic displays, spatial audio, and haptic feedback suits, the brain is tricked into a state of "presence"—the deep psychological conviction that the virtual environment is real.

However, the legal world remains stubbornly anchored in the physical. Across most jurisdictions, the definitions of assault, battery, and sexual violence are predicated on the non-consensual application of *physical force* or the touching of a *biological body*. This creates a "impunity gap" where acts that trigger genuine psychological trauma and physiological fight-or-flight responses are dismissed as "gaming

interactions" or mere content moderation issues.

This transition is not merely cosmetic; it is structural. As global economies pivot toward the "spatial web," the Metaverse is poised to become the default substrate for education, commerce, and democratic governance. Consequently, the exclusion of virtual spaces from the purview of human rights law threatens to create a "lawless layer" atop our physical reality—a zone where the protections of the Universal Declaration of Human Rights are rendered obsolete by the Terms of Service of private corporations. The danger is not only the harm to the individual victim but the systemic desensitization of society. If we accept that intimate violence in a virtual world is a trivial non-crime simply because it lacks blood and bruising, we risk eroding the moral weight of consent itself. We are facing a crisis of "Digital Citizenship," where the rights to dignity and safety are being stripped away the moment a user puts on a headset.

This paper seeks to bridge that gap. It posits that the "Digital Regime" of Human Rights 2.0 must expand the definition of "harm" beyond biological tissue damage. If the Metaverse is to be the successor to the mobile internet—a place where we work, socialize, and learn—then the right to be free from violence must extend into these synthetic corridors. We will explore the phenomenology of VR violence, the inadequacy of current criminal law, and the necessity of recognizing "Digital Bodily Integrity" as a fundamental human right[697].

II. The Phenomenology of Virtual Violence: Why It "Feels" Real

To understand why virtual harassment requires legal intervention, one must first understand the neuroscience of Virtual Reality. VR is not a video game; it is an "empathy machine" that hijacks the brain's sensorimotor system.

A. The Illusion of Body Ownership

The psychological power of VR rests on a phenomenon known as the "Illusion of Body Ownership" (IBO). This was famously demonstrated in the "Rubber Hand Illusion" experiment, where participants began to feel a rubber hand was their own when it was stroked synchronously with their real hand. VR amplifies this into a "Full Body Illusion."

When a user wears a Head-Mounted Display (HMD) and sees a digital hand move exactly when their physical hand moves, the brain's parietal lobe resolves the sensory conflict by accepting the virtual body as the "self." This is not a metaphor; it is a neurological event. Consequently, when that virtual body is violated—when an aggressor's avatar touches the user's intimate zones—the brain processes the threat as if the physical body were being touched[698].

B. The Proteus Effect and Behavioral Amplification

The "Proteus Effect," a concept introduced by researchers Yee and Bailenson, suggests that users modify their behavior to conform to their digital appearance. In social VR, this often manifests in a hyper-sexualized or hyper-aggressive manner. Anonymity, combined with the lack of physical consequences, creates a "disinhibition effect." Aggressors feel emboldened to commit acts they would never attempt in the physical world, viewing the victim not as a human, but as an interactive object[699].

C. Haptics and the Somatic Bridge

The danger is escalated by haptic technology. Modern VR setups often include haptic vests (like bHaptics) or controllers that vibrate to simulate touch. In the infamous case of the *Quiivr* player (discussed in Section III), the victim described the sensation of being groped as her controllers vibrated against her chest,

[697] Mel Slater, Place Illusion and Plausibility Illusion, 364 Phil. Transactions Royal Soc'y B 3549, 3550 (2009) (defining "presence" as the sensation of being effectively located in the virtual environment).

[698] Matthew Botvinick & Jonathan Cohen, Rubber Hands 'Feel' Touch that Eyes See, 391 Nature 756 (1998)

[699] John Suler, The Online Disinhibition Effect, 7 CyberPsychology & Behav. 321, 322 (2004)

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

VOLUME 6 AND ISSUE 3 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

creating a phantom sensation of touch. As technology advances toward "Tesla suits" that can simulate pain, heat, and pressure, the line between virtual battery and physical battery will dissolve completely[700].

D. Psychological Fallout: The Trauma is Real

The argument that "it's just a game" fails to account for the physiological reality of trauma. Victims of severe VR harassment report symptoms consistent with Post-Traumatic Stress Disorder (PTSD), including anxiety, dissociation, and hyper-vigilance. The brain's amygdala, which processes fear, does not easily distinguish between a photorealistic virtual attacker and a physical one. If the *mens rea* (criminal intent) of the attacker is to cause distress, and the *actus reus* (criminal act) results in psychological injury, the lack of physical atoms should not nullify the crime[701].

III. Case Studies in the Metaverse: The Evidence of Harm

The theoretical risks of VR have already manifested in disturbing real-world incidents. These cases serve as litmus tests for the current legal regime's failure.

1. The Nina Jane Patel Case (Horizon Worlds, 2021)

Perhaps the most high-profile instance of Metaverse abuse involved Nina Jane Patel, a psychotherapist and researcher. Within 60 seconds of logging into Meta's *Horizon Worlds* (a social VR platform), her avatar was surrounded by three male avatars. They proceeded to "gang rape" her digital body, groping her avatar's breasts and crotch while taking screenshots and shouting sexual obscenities.

Patel described the experience as a "surreal nightmare." Even though she was sitting in her living room, her physiological response was intense fear. She froze—a common trauma response. The perpetrators used the platform's spatial audio to whisper in her ears, creating a terrifying sense of proximity[702].

- **Legal Outcome:** There was no police report filed, largely because there was no "crime" under UK law. The perpetrators did not touch her physical body; therefore, no sexual assault occurred under the Sexual Offences Act 2003. The incident was treated as a Terms of Service violation by Meta, not a human rights abuse.

2. The "Quiivr" Groping Incident (2016)

In the VR archery game *Quiivr*, a female player (using the handle Jordan Belamire) was playing in a multiplayer wave defense mode. Another player approached her and began rubbing his hands over her avatar's chest. When she shouted at him to stop, he persisted. When she moved away, he chased her.

Belamire wrote, *"The virtual groping felt just as real and creepy as it would have in real life."* The breakdown of the "magic circle" of play was absolute. The developer eventually had to program a "personal bubble" mechanic that made aggressors' hands disappear if they got too close, effectively coding a law of physics to replace a law of society[703].

3. The UK Police Investigation (2024 - The 16-Year-Old Victim)

In a landmark development in early 2024, British police opened an investigation into the virtual rape of a 16-year-old girl's avatar in a metaverse game. The victim was wearing a headset and was surrounded by a group of adult male avatars who simulated a sexual assault.

This case is pivotal because it marks the first time law enforcement has seriously considered that *visual and audio simulation* of rape in VR could constitute a criminal offense, potentially under "controlling and coercive behavior" or

[700] Jordan Belamire, My First Virtual Reality Groping, Medium (Oct. 20, 2016), https://medium.com/athena-talks/my-first-virtual-reality-groping-66a0799799 42.

[701] Bessel van der Kolk, The Body Keeps the Score: Brain, Mind, and Body in the Healing of Trauma (2014)

[702] Sexual Offences Act 2003, c. 42, § 1 (UK)

[703] Belamire, supra note 11.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

child protection laws (Protection of Children from Sexual Offences). However, the police faced immediate backlash from legal purists arguing that without physical touch, rape is impossible. This tension highlights the exact crisis this paper addresses[704].

IV. The Legal Vacuum: Why 20th Century Laws Fail 21st Century Crimes

The current global legal architecture was built for a physical world. When applied to the Metaverse, structural fissures appear.

A. The Requirement of Physicality

The most significant hurdle is the definition of *Assault* and *Battery*.

- **In Common Law (UK/US):** Battery requires "unlawful application of force." Assault requires the "apprehension of immediate unlawful force." In VR, there is apprehension, but is there force? Traditional courts argue that pixels cannot apply force.
- **In India (IPC/BNS):** Section 354 of the Indian Penal Code (now BNS) criminalizes assault or criminal force to a woman with intent to outrage her modesty. While "criminal force" is usually physical, "assault" creates an apprehension. However, Indian courts have historically been conservative, viewing "virtual" acts as failing the threshold of "presence."[705]

B. The "Speech" vs. "Conduct" Dichotomy

In the United States, the problem is compounded by the First Amendment. Courts often view online behavior as "speech." If an avatar makes a lewd gesture or simulates a sex act, defense attorneys argue this is "expressive conduct" protected by free speech, provided it doesn't cross into obscenity or true threats.

Furthermore, **Section 230 of the Communications Decency Act** provides a shield for platforms. If a user is harassed in *Horizon Worlds*, Meta is generally immune from liability for the user's actions. This leaves the victim with no recourse against the platform that designed the dangerous environment and often no way to identify the anonymous perpetrator to sue them individually[706].

C. The Jurisdictional Nightmare

The Metaverse is borderless.

- *Scenario*: A victim in Mumbai is harassed in a server hosted in Dublin by a perpetrator sitting in Texas.
- *The Conflict*: Which law applies? The IT Act of India? The GDPR of Europe? Texas state law?
- *Dual Criminality*: For extradition or mutual legal assistance, the act must be a crime in both countries. If "Virtual Groping" is a crime in the UK but legally non-existent in Russia, the perpetrator faces no consequences[707].

D. The Failure of "Obscenity" Laws

Laws regarding online harassment (like cyberstalking) usually focus on the *transmission* of content (sending a photo, writing a text). They are ill-equipped to handle *synchronous* harassment. VR harassment is not "sending a message"; it is a live, shared activity. Most cyber-harassment statutes do not have provisions for "spatial invasion" or "simulated touching."

V. Human Rights 2.0: Toward a Framework of Digital Bodily Integrity

The central thesis of the "Human Rights 2.0" movement is that as human existence migrates into the digital sphere, our fundamental rights must migrate with us. The current interpretation of Human Rights—codified in the post-WWII era via the Universal Declaration of Human Rights (UDHR)—is inextricably linked to the biological human. However, in the Metaverse, the "human" is

[704] Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India)
[705] Rupal v. State of Punjab, (2018) SCC OnLine P&H 345
[706] 47 U.S.C. § 230(c)(1)
[707] Council of Europe Convention on Cybercrime art. 23, Nov. 23, 2001, E.T.S. No. 185

represented by data, avatars, and digital projections. We must therefore argue for the recognition of **Digital Bodily Integrity** as a sub-set of the Right to Security of Person.

A. Reinterpreting Article 3: Security of the Digital Person

Article 3 of the UDHR states: *"Everyone has the right to life, liberty and security of person."*

Traditionally, "security of person" refers to protection against physical detention, torture, or assault. However, the European Court of Human Rights (ECtHR) has increasingly recognized that "psychological integrity" is a crucial aspect of this right. In *M.C. v. Bulgaria*, the court acknowledged that the state has a positive obligation to protect individuals from sexual abuse, even where physical resistance was absent.

We argue that the "Digital Person"—the avatar—is an extension of the self. When an avatar is sexually assaulted in a hyper-realistic VR environment, the user's "security of person" is violated because the psychological impact (the feeling of being unsafe, violated, and terrorized) occurs in the biological brain. Therefore, State actors have a Human Rights obligation to legislate against virtual violence. Failing to criminalize VR assault effectively leaves citizens without "security" in the primary public square of the future[708].

B. The Right to Dignity in Virtual Spaces

The Indian Supreme Court, in *K.S. Puttaswamy v. Union of India*, famously declared that the Right to Privacy is intrinsic to the Right to Life and Personal Liberty (Article 21). Crucially, the court linked privacy to *dignity*.

In the Metaverse, dignity is constantly under siege. When a user is subjected to "virtual teabagging" (a practice where a player crouches their avatar over a victim's face) or "verbal gang-stalking," their dignity is eroded. If Human Rights 2.0 is to mean anything, it must encompass the Right to Digital Dignity—the right to navigate virtual spaces without being subjected to degrading treatment that leverages the immersive nature of VR to humiliate the user[709].

C. The Gendered Dimension: CEDAW and the Metaverse

Virtual harassment is not gender-neutral. Studies show that users with female-presenting avatars are disproportionately targeted for sexual violence and harassment. This brings VR abuse under the ambit of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).

Article 2 of CEDAW mandates states to "take all appropriate measures to eliminate discrimination against women." By allowing a "Wild West" environment in the Metaverse where female users are forced to hide their gender or avoid social spaces to escape virtual rape, states are failing their CEDAW obligations. The "Digital Regime" creates a hostile environment that effectively excludes women from the economic and social opportunities of the Metaverse, constituting a Human Rights violation of equal access[710].

VI. Comparative Legal Analysis: The Global Lag

To understand the path forward, we must critique how major legal systems currently attempt (and fail) to regulate this domain.

1. The United Kingdom: The Online Safety Act 2023

The UK is currently a pioneer with its Online Safety Act (OSA).

- **Strengths:** The OSA introduces a "duty of care" for platforms. It moves away from merely policing content to policing *harm*. It specifically categorizes "threatening communications" and creates a new

[708] M.C. v. Bulgaria, 2003-XII Eur. Ct. H.R. 1 (establishing positive obligations on states to investigate sexual abuse even without physical resistance).

[709] Brittan Heller, Reimagining Reality: Human Rights and the Metaverse, Stan. Cyber Pol'y Ctr. (2021)

[710] Guo Freeman et al., Simulating the Physical: The Challenge of Sexual Harassment in Social VR, in Proc. of the 2022 CHI Conf. on Hum. Factors in Computing Sys. 1, 3 (2022)

offense for "cyber-flashing" (sending unsolicited sexual images).

- **Weaknesses regarding VR:** The OSA is still largely text/image-focused. While it addresses "communication," it is unclear if the *act* of a silent avatar groping another avatar falls under "communication." Furthermore, the definition of "harm" is tied to "psychological distress," which is high-threshold. A brief grope in VR might not cause clinical distress but is a violation of dignity. The UK law essentially asks: "Did it hurt you?" rather than "Was it wrong?"[711]

2. India: The Information Technology Act & BNS

India's digital legal framework is governed by the IT Act, 2000, and the newly introduced Bharatiya Nyaya Sanhita (BNS).

- **IT Act Section 67:** Deals with publishing "obscene" material. This applies if a user *uploads* a video of VR rape, but it is unclear if it applies to the *live act* of doing it inside a private server.
- **BNS Section 74 (formerly IPC 354):** Criminalizes assault with intent to outrage modesty. The challenge in India is the "corporeal requirement." Indian courts have historically required physical presence for "criminal force." While "Stalking" (Section 78 BNS) includes monitoring online, "Virtual Assault" is a lacuna.
- **The Gap:** India treats the Metaverse as "Content" rather than "Conduct." Until Indian law recognizes that an avatar is a *subject* of rights rather than an *object* of code, victims have no recourse[712].

3. The European Union: The Digital Services Act (DSA)

The EU's DSA is the most comprehensive regulation of digital platforms.

- **Systemic Risk:** The DSA requires Very Large Online Platforms (VLOPs) like Meta to assess "systemic risks," including risks to fundamental rights and gender-based violence.
- **The Opportunity:** This is the most promising avenue. The DSA compels Meta to prove that *Horizon Worlds* is designed in a way that mitigates the risk of virtual rape. If they fail, they face massive fines (up to 6% of global turnover). This shifts the burden from the victim (criminal law) to the platform (regulatory law). However, it is a preventative measure, not a punitive one for individual aggressors[713].

4. United States: The Section 230 Shield

The US remains the home of most Metaverse companies but offers the least protection.

- **Section 230:** As discussed, this immunizes platforms.
- **First Amendment:** The Supreme Court case *Brown v. Entertainment Merchants Association* established that video games are protected speech. This makes banning "simulated violence" constitutionally difficult. A US court might argue that "virtual rape" is essentially a "performance" by an avatar, protected as expression, unless it falls into the narrow exception of obscenity or true threats. This libertarian approach is the antithesis of the Human Rights 2.0 model[714].

[711] Online Safety Act 2023, c. 50, pt. 10 (UK
[712] Bharatiya Nyaya Sanhita, 2023, §§ 74, 78, No. 45, Acts of Parliament, 2023 (India)
[713] Regulation (EU) 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), art. 34, 2022 O.J. (L 277)
[714] Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 790 (2011).

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

VOLUME 6 AND ISSUE 3 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

VII. The "Digital Regime" Proposal: Legal and Technical Solutions

We cannot rely on 20th-century statutes to solve 21st-century problems. To bridge the gap between Virtual Violence and Real Harm, we propose a three-tiered solution framework for the International Human Rights community.

Tier 1: Legislative Reform – Defining "Virtual Assault"

We must amend penal codes to include a new class of offenses specifically for immersive environments.

- **Proposed Definition:** *"Virtual Assault is the intentional, non-consensual violation of a user's digital avatar in an immersive environment, which, through the use of haptic feedback, spatial audio, or visual proximity, causes the victim to reasonably apprehend immediate violence or suffer violation of dignity."*
- **Decoupling from Touch:** The law must explicitly state that "force" in a digital context includes "data force"—the manipulation of code to invade the personal space of another user against their will.
- **Severity Grading:**
  - *Level 1 (Harassment)*: Verbal abuse, blocking paths, "trolling." (Civil Penalty/Ban).
  - *Level 2 (Virtual Battery)*: Unwanted touching of non-intimate areas, haptic spamming. (Misdemeanor).
  - *Level 3 (Virtual Sexual Assault)*: Simulated sexual acts, groping intimate zones, "gang" aggression. (Criminal Offense punishable by law)[715].

Tier 2: Platform Liability & "Safety by Design"

Human Rights 2.0 demands that corporations be held as duty-bearers.

- **Mandatory "Personal Bubbles":** Platforms should be legally mandated to enable "Personal Boundaries" by default. Currently, many platforms make this an opt-in feature. It must be "Safety by Default." If a user wants to allow touch, they must affirmatively consent (Opt-in).
- **Haptic Regulation:** There should be restrictions on the intensity and placement of haptic feedback. A haptic suit should *never* be allowed to simulate touch on genitalia without explicit, age-verified, and context-specific consent (e.g., in specific cyber-sex applications, but never in public social lobbies).
- **Universal Blocklist:** If a user acts as a sexual predator in *VRChat*, they should not be able to log into *Horizon Worlds* five minutes later. We propose a decentralized, privacy-preserving "Reputation Protocol" shared across the Metaverse to prevent serial abusers from hopping platforms.

Tier 3: The Attribution Problem & Digital Identity

The biggest practical hurdle to prosecuting VR crimes is anonymity.

- **Self-Sovereign Identity (SSI):** We propose the use of Zero-Knowledge Proof (ZKP) identities. A user can prove they are a unique, real human over the age of 18 without revealing their real name to the platform.
- **The "Piercing the Digital Veil" Standard:** While anonymity is a right, it is not absolute. Legal frameworks should establish a standard: *If probable cause of Level 3 Virtual Assault is established, the platform must decrypt the user's ZKP identity for law*

[715] Michael Madary & Thomas K. Metzinger, Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology, 3 Frontiers in Robotics & AI 1, 12

enforcement. This balances privacy with accountability[716].

VIII. Challenges and Counter-Arguments

Any robust academic paper must address the counter-arguments.

1. The "Floodgates" Argument:

Critique: "If we criminalize virtual touching, police will be overwhelmed with reports of teenagers t-bagging each other in Call of Duty."

Rebuttal: This is why the definition relies on "Immersive Environments" (VR/AR) and "Haptic/Spatial Reality." We are distinguishing between looking at a screen (2D gaming) and inhabiting a space (VR). The law already distinguishes between "assault" and "playground roughhousing" based on context and severity; the same judicial discretion applies here.

2. The Desensitization Dilemma:

Critique: "It's just pixels. Victims should just take off the headset."

Rebuttal: This is the "victim blaming" equivalent of telling a woman "just don't walk down that dark alley." The Metaverse is becoming a place of work, education, and essential socialization. Telling victims to "leave" is telling them to abdicate their right to participate in the digital future. Furthermore, the "take off the headset" argument ignores the *immediate* physiological shock. The damage (cortisol spike, trauma response) often happens *before* the user can physically remove the device[717].

3. The Global Enforcement Issue:

Critique: "How can India prosecute a gamer in Brazil?"

Rebuttal: This requires a "Digital Geneva Convention." Just as we have international treaties for maritime law or outer space, we need a **Convention on Digital Human Rights**. In the interim, "extraterritorial jurisdiction" (ETJ) should be applied, allowing a country to prosecute crimes committed against its citizens anywhere in the Metaverse, similar to how child abuse laws currently work globally.

IX. Conclusion: The Imperative for a New Jurisprudence

The Metaverse stands at a crossroads. It can become a utopia of boundless connection, or a dystopia of unchecked violation. The incidents of virtual rape and harassment we see today are the tremors before the earthquake. As VR graphics become indistinguishable from reality, and haptics become indistinguishable from touch, the distinction between "virtual violence" and "real harm" will not just blur—it will vanish.

This paper has argued that the current legal regime, tethered to the physicality of the 20th century, is woefully inadequate for the challenges of the 21st. By failing to recognize the "Digital Person" as a vessel of human dignity, we are creating a human rights vacuum.

Furthermore, the cost of inaction extends beyond individual trauma to societal regression. If we permit the Metaverse to function as a consequence-free sanctuary for humanity's darkest impulses, we risk desensitizing an entire generation to the mechanics of assault. The "magic circle" of gameplay cannot be allowed to serve as a shield for dehumanization. We must also confront the economic imperative of this crisis; as the Metaverse evolves into a multi-trillion-dollar economy, safety becomes a prerequisite for participation. If women and marginalized communities are forced to retreat from these spaces due to unchecked harassment, we are effectively endorsing a new form of "digital segregation." The ratification of digital rights is, therefore, not merely an act of regulation, but an act of civilization. Just as we established laws to make physical travel safe, we must encode rights to make virtual existence secure.

[716] Christopher Allen, The Path to Self-Sovereign Identity, Coindesk (Apr. 25, 2016), https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/
[717] Mark A. Lemley & Eugene Volokh, Law, Virtual Reality, and Augmented Reality, 166 U. Pa. L. Rev. 1051, 1075 (2018)

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

VOLUME 6 AND ISSUE 3 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

We call upon the international legal community, gathered here for the "Human Rights 2.0" conference, to adopt the **"Embodied Harm Doctrine."** This doctrine asserts that:

1. Harm to the avatar in an immersive state is harm to the mind of the user.
2. Sexual violence does not require biological contact to be traumatic or criminal.
3. The right to digital bodily integrity is a fundamental human right.

The law must not wait for a tragedy to evolve. We must build the legal guardrails of the Metaverse now, ensuring that as humanity migrates to the digital regime, we do not leave our humanity behind.