Beyond the Avatar: Horizontal Application of Fundamental Rights to Metaverse Platforms in India

AI Disclosure Statement:

The author used AI-assisted tools only to improve language, grammar, and readability. The research conducted, the legal arguments, analysis of authorities and case law, and the conclusions reached in this manuscript are the sole responsibility and work of the author.

Abstract

Virtual reality, or the "metaverse", is an emerging issue for legal governance. In the current landscape, private entities in the form of technology companies are able to shape users' behaviour, personal information, and online identity without the same constitutional obligations as those of the State. In this study, the question is whether such platforms can be regulated under the Indian constitutional law doctrine of "horizontal application". There was a traditional understanding that Articles 19 and 21 of the Constitution would be enforced primarily against the State and its instrumentalities, as defined under Article 12.[1]

This shift is due to the concurring opinion of Justice Kaul in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) in which it was held that the right to privacy also has to be safeguarded against non-State actors, especially in the event of large-scale private data collection.[2] The Supreme Court's majority judgment in *Kaushal Kishor v. State of Uttar Pradesh* (2023), reaffirming the direct horizontal application of Articles 19 and 21, further bolstered this development.[3]

The paper argues the horizontal approach provides a sound constitutional basis for extending fundamental rights protection to metaverse users, though it still lacks the legislation and institutional mechanisms needed for effective implementation.

Keywords: Metaverse, Horizontal Application, Fundamental Rights, Right to Privacy, Data Protection.

[1]INDIA CONST. art. 12.
[2]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India) (Kaul, J., concurring).
[3]*Kaushal Kishor v. State of Uttar Pradesh*, (2023) 4 SCC 1 (India).

1. Introduction

The Metaverse represents a significant shift in the creation, experience, and governance of digital space. The metaverse is different from the early days of the internet, which was primarily a place for communication and information sharing, because it renders persistent and immersive worlds where people can socialise, play, work, and do economic transactions using avatars. But most of these areas are privately owned and managed. The design, use, content policies, and data management of technology companies are self-determined. This means that the private platforms have a high degree of influence over the behaviour, communication, and presentation of the people who choose to use them in these virtual spaces. An important question of constitutional accountability thus arises. The rules governing what is allowed, what can be taken down, what information can be gathered and how that information is used to monitor users' digital identity and behaviour are subject to the discretion of platform operators. Private platforms can assert some control over content through end-user license agreements, content moderation, targeted advertising, and data collection, in ways that can be likened to those of public authorities.

But the constitutional restrictions generally do not apply to private parties as they do to the State. The problem is more complicated in the old interpretation of Part III of the Constitution. The main focus of fundamental rights has been against the State, and against authorities within the scope of Article 12, mostly vertically.[4] The government can therefore generally be held to account for its actions only if they are connected with the exercise of governmental power. Therefore, private entities are generally not subject to constitutional review, even though their actions can significantly affect the exercise of individual rights. However, in the metaverse, this separation is blurring. Behavioural tracking, data collection via surveillance, discriminatory design, avatar harassment, and manipulative engagement mechanisms are ways that privacy and personal liberty, freedom of expression, and autonomy can be threatened or compromised. The question then is whether constitutional protection can have a horizontal dimension when fundamental rights are involved in the actions of a private individual. The decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* reaffirmed the importance of the right to privacy in

[4]INDIA CONST. art. 12.

safeguarding individual autonomy and personal information in a digital age.[5] The judgment also offers valuable insights for the analysis of the role of non-State parties.

Likewise, the debate on the horizontal application of fundamental rights and the relationship between Articles 19 and 21 with private actors was influenced by *Kaushal Kishor v. State of Uttar Pradesh*.[6] Keeping this in mind, this paper considers whether horizontal application can offer constitutional justification for holding private metaverse platforms accountable when their practices have a material impact on users' rights under Ar. It highlights the issues associated with data extraction, content control, digital identity and user behaviour, and also the lack of a specific regulatory framework that is designed for the metaverse in India. The paper suggests that constitutional principles, together with suitable legislation and institutional arrangements, can offer a meaningful basis for ensuring protection of individuals in the domain of private control.

2. The Metaverse Governance Problem

The metaverse is essentially a private technology space, and not a public institution. These companies design the technical structure, set the guidelines by which users can interact, define virtual property, and define the terms and conditions that have to be accepted to access the platform. Compared to public places, users rarely have a chance to share in the creation of such rules. What emerges is a world of digital space in which private institutions have an important say in the ways in which people communicate, interact, and present themselves. As avatars are the key to the user's experience in the metaverse, choices around the avatar and its context can directly affect the user who created it. This is a type of private governance that poses a number of concerns.

The first one is data extraction and privacy. Unlike online platforms, metaverse platforms can gather much more personal data about their users, such as eye movements, gestures, body movements, biometric data and user behaviour. A lot of this data can be gathered on an ongoing basis and utilised for business goals such as targeted marketing and behavioural profiling. The issue is not only about gathering the data, but also the ability of the immersive technologies to provide continuous monitoring of persons. The second is in regard to dignity and the user's personal security. Bad behaviour, whether it means stalking or verbally abusing another user, interacting with an avatar without their consent, or

[5] *Puttaswamy*, (2017) 10 SCC 1 (India).
[6] *Kaushal Kishor*, (2023) 4 SCC 1 (India).

deliberately excluding another user from the experience, can cause real-world problems for users, even if all interaction takes place virtually. Moderation systems in place may fail to offer timely and effective remedies to this behaviour in all instances. Addictive and manipulative design are a third area of concern. Rewards, the need to keep coming back to platforms, and engaging with sensory information can help encourage users to spend a lot of time on platforms. This can be of specific concern when minors or other vulnerable users are involved.

The fourth concern is discrimination and exclusion. The representation of avatars, their accessibility, the content recommended to each user, and the design of the platforms can reproduce social biases or exclude users who fall outside the assumptions of platform designers. The concerns show that the metaverse cannot be considered solely as a contractual relationship between a platform and its users. A contractual approach could justify the practices of the platform on the basis of the user's acceptance of the terms of service. Some modes of information gathering, limitations on expression and behaviour that impact personal dignity, however, do escalate interests safeguarded by fundamental rights. There is a close connection between privacy and dignity as they relate to Article 21, and expression in digital environments may engage Article 19(1)(a).[7] The central challenge, then, is how to allow for constitutionally relevant harms to be inflicted by private actors. Such a disconnect between the nature of the harm and the identity of the actor offers a starting point for discussing the possibility of horizontal application of fundamental rights in relation to private metaverse platforms.

3. The Horizontal Application Doctrine

3.1 Traditional Vertical Application

Traditionally in India, fundamental rights have been interpreted as rights of the individual against the State, which are vertical rights. This is connected to Article 12, which states that 'The State' shall include the Government and Parliament of India, State Governments and Legislatures, local or other authorities.[8] In general, where someone claims a fundamental rights violation, they would need to demonstrate that the State or its agents under Article 12 were responsible. Instead, private conduct was regulated by ordinary law, namely the laws of contract, tort and other private law areas, rather than by Part III. But

[7]INDIA CONST. arts. 19(1)(a), 21.
[8]INDIA CONST. art. 12.

there has never been an absolute division between State and private action. Some parts of the constitution already directly constrain private persons. There is discrimination in access to public places even when it is by a private party (Article 15(2)); untouchability is prohibited (Article 17); and trafficking and forced labour are prohibited (Article 23).[9] The fact that these provisions demonstrate that the Constitution can and does direct private behaviour when it is of substantial importance is significant. But, beyond the question of whether rights can be exercised horizontally, what are the rights that can be and how can they be exercised?

3.2 The Doctrinal Shift: From *Puttaswamy* to *Kaushal Kishor*

The developing right to privacy can answer this question. The Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) had unanimously declared privacy as a fundamental right.[10] The separate opinion of Justice Sanjay Kishan Kaul is particularly important for the discussion on the horizontal application of the judgment as he noted that there is not just the State, but private parties too that have a lot of power to collect, process and use personal data, which is threatening privacy.[11] This logic created a space for the notion that constitutional protection of individual liberty should not be limited to the boundaries of the State, and that has increased as the power of digital platforms has become an influence on privacy, speech, reputation and autonomy, similar to the power of State actors. This led to *Kaushal Kishor v. State of Uttar Pradesh* (2023), where for the first time a five-judge Constitution Bench of the Supreme Court addressed the question of whether rights under Articles 19 and 21 could be enforced against non-State actors.[12] The majority answered this question in the affirmative.

The case applied to the Minister's comments relating to a criminal incident and the questions referred related to the horizontal application of Articles 19 and 21 and whether restrictions on freedom of speech could be based on other fundamental rights. The point of the majority that was most worth noting on Article 21 is that the word 'State' does not appear in Article 21, and therefore the right to life and personal liberty is not limited to State action alone.[13] The State, however, has a positive obligation to keep people safe,

[9] INDIA CONST. arts. 15(2), 17, 23.
[10] *Puttaswamy*, (2017) 10 SCC 1 (India).
[11] Id. (Kaul, J., concurring).
[12] *Kaushal Kishor*, (2023) 4 SCC 1 (India).
[13] Id.

which also includes protection from private individuals, and the possibility of such extension of Article 21 is not excluded.

3.3 Scope and Application of Horizontal Rights in the Metaverse

This represents a major transformation, though not without its flaws. The judgment does not do away with the public/private distinction. Justice B.V. Nagarathna disagreed on the horizontal interpretation, stating that Articles 19 and 21 were essentially vertical with certain exceptions, like habeas corpus, and distinguishing between a fundamental right and an equivalent right available under the ordinary law.[14] Some commentaries, as a result of its context in a narrow factual setting -- a Minister's statement -- have suggested it be read narrowly: that is, as a complaint over ministerial accountability rather than broadly as a right to make horizontal claims against any private person.[15] The majority also failed to define the boundaries, relief, or rules to govern horizontal enforcement, an omission that has received some fair criticism in the academic world because otherwise a constitutional adjudication of every private dispute would be permitted under Part III of the Constitution. Nonetheless, the meaning of a judgment is not just in what it says about the facts, but in the principle it sets; and the Constitution Bench clearly questioned and answered as to whether or not Articles 19 and 21 extended to non-State actors. *Kaushal Kishor* is better read as opening a constitutional door as opposed to giving unlimited license to litigate private disputes as fundamental rights claims. Its reasoning seems to be the most compelling in cases where there is a significant private interest involved in the decision-making that affects interests of Articles 19 and 21 and where ordinary legal remedies are inadequate to compensate for the harm.

The key factor here, from this perspective, is not the distinction between public and private but what type of right is at stake, how much private power is at play, how serious the interference is, and how secure the legal protections are. This is especially suitable for the metaverse. The ownership of these platforms is private, but so are the various aspects of users' access to them, their level of freedom of speech, who can join, what kind of personal information is collected, how it is processed, and even whether users' digital

[14] *Kaushal Kishor*, (2023) 4 SCC 1 (India) (Nagarathna, J., dissenting).
[15] Gautam Bhatia, *Kaushal Kishor, Horizontal Rights, and Free Speech: Glaring Conceptual Errors*, Indian Constitutional Law and Philosophy (Jan. 27, 2023, 5:18 PM IST), https://indconlawphil.wordpress.com/2023/01/27/kaushal-kishor-horizontal-rights-and-free-speech-glaring-conceptual-errors/ (on file with author) (last visited Sept. 15, 2026).

identity or social life after they leave the platform lives on or is obliterated, depending on the platform's design.

Assuming these entities are only private contracting parties may well be minimising the true relationship between platform and user. The horizontal application doctrine is then a useful analytical tool for the Constitution in the context of private power in digital space. *Puttaswamy* first recognised that constitutional privacy is a frame that needs to be sensitive to non-State power, and *Kaushal Kishor* applied this to the enforceability of privacy.

Applying Horizontal Rights to Metaverse Platforms

The doctrinal foundation discussed above becomes significant only when applied to concrete forms of private digital power. The question, therefore, is what it would mean in practice to subject metaverse platforms to Article 21 standards, notwithstanding that Article 21 was not originally framed with private corporations in mind. Three categories of platform conduct are particularly relevant: the collection of data from avatar behaviour, tracking that operates at the intersection of biometric and behavioural data, and dignitary harm arising from avatar-based harassment.

Avatar movement generates a continuous stream of behavioural data. Every movement, hesitation, change in direction, or reaction to a stimulus may be recorded by the platform. Such data may be more revealing than information collected by conventional text-based platforms because it can capture involuntary and semi-conscious behaviour rather than deliberate disclosure. Justice Kaul's opinion in *Puttaswamy*[16] treated granular behavioural information as central to informational privacy because it can reveal aspects of an individual that they may not consciously choose to disclose. Where a metaverse operator uses such data to construct predictive profiles for advertising or engagement optimisation, the underlying privacy concern remains similar to that identified in *Puttaswamy*.[17] The principal difference is that the data is collected by a private corporation rather than the State. A meaningful application of horizontal rights would therefore require this distinction to become less decisive where private actors exercise comparable power over individual autonomy.

[16] *Puttaswamy*, (2017) 10 SCC 1 (India) (Kaul, J., concurring).
[17] Id.

A related concern arises where tracking falls outside existing definitions of biometric data while producing comparable effects. Eye-tracking for rendering efficiency, hand and gesture tracking for controls, and, in advanced devices, the collection of heart rate or facial micro-expressions for enhanced immersion can enable platforms to identify individuals or infer emotional states with a degree of precision unavailable from ordinary data. The concern consequently extends beyond informational privacy to bodily and psychological autonomy, areas closely connected with Article 21. Reliance on consent contained within lengthy and largely unread terms-of-service agreements raises concerns regarding the meaningfulness of such consent. A rights-based framework that reduces the inquiry to the existence of a checkbox risks overlooking the substantive nature of the interference.

Avatar-based harassment presents a further dimension of the problem, including simulated groping, non-consensual proximity, stalking and targeted abuse within virtual environments. Such incidents have already been reported on major metaverse platforms, demonstrating that the resulting psychological and dignitary harm cannot necessarily be dismissed as merely virtual. Article 21's protection of dignity has not been confined to physical integrity, particularly following the broader understanding of life and personal liberty developed in *Maneka Gandhi*.[18] There is therefore a doctrinal basis for recognising serious forms of virtual harm within the constitutional conception of dignity. Horizontal application further raises the question of platform responsibility: not merely who perpetrated the harassment, but whether the platform's design, governance and commercial incentives contributed to creating and sustaining the environment in which such conduct occurred.

Article 19(1)(a) is also relevant, although comparatively secondary to the Article 21 concerns.[19] Expression through avatars and the moderation of such expression by metaverse platforms implicate constitutional interests in freedom of speech. Where moderation practices are inconsistent, opaque or primarily driven by commercial considerations rather than coherent standards, horizontal application provides a possible basis for examining such decisions as constitutional questions rather than matters governed exclusively by private terms of service. Nevertheless, the principal constitutional concern remains the protection of privacy, dignity and autonomy under Article 21.

[18] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).
[19] INDIA CONST. art. 19(1)(a).

The need for such a doctrinal approach is reinforced by the limitations of India's existing statutory framework. The Information Technology Act, 2000 was enacted to address a substantially different technological environment. Section 66E criminalises the capture or publication of images of a person's private areas, presupposing a form of photographic conduct that does not readily correspond to avatar-based harassment.[20] Section 66C addresses identity theft through the fraudulent or dishonest use of passwords or other identifying features, offering an imperfect fit for the appropriation or manipulation of a person's digital persona through an avatar.[21] Similarly, Sections 67 and 67A regulate obscene and sexually explicit electronic material, requiring metaverse conduct to be brought within categories developed for conventional forms of digital content.[22] Such provisions may, in certain circumstances, be applied by analogy, but this approach remains uncertain and dependent upon judicial interpretation, thereby limiting predictability for users.

The Digital Personal Data Protection Act, 2023 was intended to address several deficiencies in India's data-protection framework. However, its phased commencement means that, as of 2026, the framework has not yet become fully operational.[23] Consequently, provisions concerning matters such as meaningful consent, purpose limitation and the enforcement functions of the Data Protection Board cannot yet provide a complete safeguard against all forms of platform-related harm. This regulatory gap strengthens the case for horizontal fundamental-rights protection as an interim constitutional mechanism. Such protection need not operate as a permanent substitute for legislation; rather, it can function as a constitutional bridge while statutory law develops in response to technological changes that have already transformed the nature of privacy, autonomy, dignity and expression in digital spaces.

[20]The Information Technology Act, 2000, No. 21 of 2000, § 66E (India).
[21]Id. § 66C.
[22]Id. §§ 67, 67A.
[23]The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India); Ministry of Electronics & Info. Tech., *DPDP Rules, 2025 Notified*, Press Information Bureau (Nov. 17, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf (on file with author) (last visited Sept. 15, 2026) (Rules notified on 14 November 2025, with an eighteen-month phased compliance period).

4. Conclusion

The concept of horizontal application of fundamental rights to metaverse platforms is promising but not without issues. In order for constitutional protection to be meaningful in the metaverse, these practical and doctrinal hurdles must be addressed. First and foremost, there is an enforcement issue. The constitutional remedies under Articles 32 and 226 are there, but normally writ jurisdiction is against the State or an authority within the ambit of the State.[24] It is not sufficient to merely state that there are "constitutional obligations" placed on a private metaverse platform to fully appreciate how a user can enforce such obligations.

A second question left unaddressed by *Kaushal Kishor* is whether Articles 19 and 21 provide an individual with a direct cause of action against a private entity or whether they are primarily an interpretation of the existing causes of action available under contract, tort, and statutory law.[25] This distinction is relevant in the real world. When one avatar sexually harasses another, for instance, it may have been the platform that enabled it, but it's not necessarily the one who did the actual harassing. The issue then is whether it is the individual user's responsibility, the platform's responsibility for failing to protect or react to the conduct, or both. The cross-border aspect of metaverse platforms complicates the situation further.

A number of the platforms that could be party to such conflicts may be foreign entities. This may lead to doubts regarding territorial jurisdiction, service of proceedings and most significantly, whether a decision issued by an Indian court can be enforced against the platform. A right without a means of enforcement is of limited utility to the person who would be the beneficiary of the right.[26]

Also, some doubt the doctrinal calibre of *Kaushal Kishor*. The decision was not unanimous, and its discussion of horizontal application of Articles 19 and 21 offers no detailed explanation of the limits of that application.[27] In the future, a larger Bench might read the decision as narrowly as it was written, or broaden the scope of constitutional rights by further interpreting that they only work against a private actor primarily through other laws. Thus, judicial protection may be an interim measure of protection, and also be

[24]INDIA CONST. arts. 32, 226.
[25]*Kaushal Kishor*, (2023) 4 SCC 1 (India).
[26]Bhatia, supra note 15.
[27]*Kaushal Kishor*, (2023) 4 SCC 1 (India) (Nagarathna, J., dissenting).

a call for legislative reform. The goal is not to turn constitutional law into a solution to a lack of legislation, but to ensure that fundamental rights are not without a remedy.

Bibliography

- **Constitutional Provisions**

INDIA CONST. art. 12.

INDIA CONST. art. 15(2).

INDIA CONST. art. 17.

INDIA CONST. art. 19(1)(a).

INDIA CONST. art. 21.

INDIA CONST. art. 23.

INDIA CONST. art. 32.

INDIA CONST. art. 226.

- **Cases**

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

Kaushal Kishor v. State of Uttar Pradesh, (2023) 4 SCC 1 (India).

Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).

- **Statutes**

The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

The Information Technology Act, 2000, No. 21 of 2000 (India).

- **Secondary and Internet Sources**

Gautam Bhatia, *Kaushal Kishor, Horizontal Rights, and Free Speech: Glaring Conceptual Errors*, Indian Constitutional Law and Philosophy (Jan. 27, 2023, 5:18 PM IST), https://indconlawphil.wordpress.com/2023/01/27/kaushal-kishor-horizontal-rights-and-free-speech-glaring-conceptual-errors/ (on file with author) (last visited Sept. 15, 2026).

Ministry of Electronics & Info. Tech., *DPDP Rules, 2025 Notified*, Press Information Bureau (Nov. 17, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025111769 5301.pdf (on file with author) (last visited Sept. 15, 2026).