

Protecting Human Dignity in the Digital Age: A Critical Study of India's Humanitarian Law Framework and Data Protection Regime in Conflict, Crisis, and Displacement Contexts

Dr. Himanshi Babbar¹ Dr. Nishi Kant Bibhu² Dr. Shivam Gaur³

Introduction

In the digital age, the governance of personal data has emerged as one of the most pressing legal and ethical questions confronting contemporary states. This challenge becomes especially acute in situations of conflict, crisis, and displacement, where individuals are compelled to interact with humanitarian institutions, state authorities, and digital systems at moments of extreme vulnerability. In such contexts, the collection and processing of personal information is rarely a neutral administrative exercise; rather, it directly affects access to relief, protection, identity, mobility, and survival. The protection of personal data in humanitarian settings is therefore inseparable from the protection of human dignity. The International Committee of the Red Cross has expressly recognized that safeguarding personal data is integral to safeguarding life and dignity in humanitarian action (ICRC, 2024).

India's transition toward a digitally mediated governance model has intensified the importance of this issue. The enactment of the Digital Personal Data Protection Act, 2023 marks a significant statutory effort to regulate the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need for lawful processing (Digital Personal Data Protection Act, 2023). While this legislation establishes a formal framework for consent, legitimate use, data principal rights, and institutional oversight, its general architecture does not fully account for the unique pressures that arise in humanitarian environments. Crisis-affected persons often have limited autonomy, reduced

bargaining power, and little practical ability to refuse data collection when assistance is contingent upon disclosure. In such circumstances, the ordinary assumptions underlying consent-based privacy regulation are weakened, if not entirely displaced.

The constitutional dimension of privacy in India further strengthens the normative basis of this inquiry. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court held that privacy is intrinsic to human dignity and an essential attribute of liberty under Article 21 (Puttaswamy v. Union of India, 2017). The Court also affirmed that any invasion of privacy must satisfy the tests of legality, legitimate state aim, and proportionality (Puttaswamy v. Union of India, 2017). These principles are particularly relevant in humanitarian settings, where state intervention is often justified by the urgency of relief, public welfare, or administrative efficiency. Yet the very urgency that makes humanitarian intervention necessary may also increase the risk of excessive data collection, profiling, and surveillance. The question, therefore, is not merely whether the state or aid provider has a legal basis for processing personal data, but whether such processing remains proportionate, necessary, and consistent with dignity.

Humanitarian law, in its classical form, is concerned with the protection of persons in situations of armed conflict and comparable emergencies. However, the digitisation of humanitarian operations has introduced new risks that traditional humanitarian norms do not always address with sufficient precision. Relief systems increasingly depend on biometric identification,

¹Assistant Professor of Law, Vivekananda Institute of Professional Studies, GGSIPU.

²Assistant Professor of Law, School of Law, Bennett University.

³Assistant Professor of Law, School of Law, Bennett University.

digital registries, online registration platforms, and algorithmic decision-making tools. These technologies can enhance efficiency, reduce duplication, and improve targeting of aid, but they can also produce exclusion, discriminatory profiling, data breaches, and long-term informational harm. The ICRC's Handbook on Data Protection in Humanitarian Action notes that humanitarian organizations must ensure compliance with data protection standards, especially when new technologies are employed in volatile environments and for the benefit of highly vulnerable populations (ICRC, 2024). This reinforces the need to examine humanitarian data governance not as a technical matter alone, but as a core rights issue.

The Indian legal landscape is especially significant because it sits at the intersection of constitutional privacy, digital governance, welfare administration, and emergency response (Bibhu & Dubey, n.d.). India has witnessed large-scale internal displacement due to conflict, communal violence, environmental degradation, industrial disasters, and natural calamities. In many such settings, relief and rehabilitation are increasingly mediated through data-driven systems. While digital platforms may improve coordination, they also concentrate sensitive information in the hands of state and non-state actors. Without strict legal safeguards, such information may be reused beyond the original purpose, shared without meaningful transparency, or exposed to cyber and administrative misuse. For displaced or crisis-affected persons, such harms are not abstract; they can determine whether assistance is received fairly, whether identity is preserved, and whether personal safety is maintained.

This study therefore adopts a critical and interdisciplinary approach to examine whether India's humanitarian law framework, read together with its data protection regime, is capable of adequately protecting individuals in conflict, crisis, and displacement contexts. It asks whether existing legal norms sufficiently regulate the collection, storage, transfer, and use of personal data in emergencies, and whether current safeguards meaningfully reflect the constitutional value of dignity. The central argument is that humanitarian relief cannot be permitted to become

a site of informational vulnerability. Rather, humanitarian action in the digital age must be governed by principles of necessity, proportionality, accountability, purpose limitation, and contextual sensitivity. A legal framework that fails to account for these values risks turning protection into exposure.

Accordingly, this paper contends that India requires a more context-specific model of humanitarian data governance. Such a model should not treat personal data merely as an administrative resource, but as an extension of the individual's dignity, autonomy, and security. By bringing humanitarian law and data protection law into the same analytic frame, this study seeks to contribute to the development of a more humane, technologically aware, and rights-centered legal framework for crisis governance in India.

Humanitarian Law, Conflict, Crisis, and Displacement in India

Humanitarian law, when viewed in the Indian context, is not confined to conventional battlefields. It becomes relevant wherever organized violence, internal disturbances, mass displacement, emergency relief, and state responses to crisis create conditions in which the dignity, safety, and survival of persons are placed at risk (ICRC, 2019). In India, this relevance is especially visible in regions affected by insurgency, communal violence, border tensions, natural disasters, and large-scale internal migration, where the protection of vulnerable populations requires a legal lens that goes beyond ordinary administrative governance (India's Engagement with International Humanitarian Law, 2024). India's engagement with international humanitarian law is rooted in its constitutional authority to implement treaty obligations and in the Geneva Conventions Act, 1960, which gives domestic effect to core humanitarian commitments.

Conflict in India does not always assume the form of formally declared war, yet humanitarian concerns arise whenever civilians are exposed to violence, coercive security operations, or conditions of prolonged insecurity. International humanitarian law was designed to regulate conduct

in armed conflict and to protect those who are not, or are no longer, participating in hostilities (ICRC, 2019). In the Indian setting, this protection is particularly significant in disturbed areas where civilian life is disrupted and where the line between security imperatives and humanitarian obligations can become blurred. Scholarship on India's relationship with humanitarian law has repeatedly noted the difficulty of applying international humanitarian law to internal conflicts, especially because India has not recognized Additional Protocol II, which specifically addresses non-international armed conflicts (Analysing International Humanitarian Law in the Indian Context, 2023).

The crisis dimension of this topic is equally important. Humanitarian crises in India often emerge not only from armed conflict but also from disasters, public health emergencies, and state responses to instability. During such periods, individuals may lose access to housing, livelihood, healthcare, documentation, and personal security. When crisis conditions become prolonged, legal questions arise concerning relief distribution, rehabilitation, personal liberty, and state accountability. The humanitarian value of legal protection lies in its capacity to ensure that emergency governance does not reduce people to objects of administration. Instead, law must remain attentive to the personhood of those affected, especially where vulnerability is intensified by poverty, gender, caste, disability, or geographic isolation (India's Engagement with International Humanitarian Law, 2024).

Displacement is one of the most visible consequences of conflict and crisis in India. Internally displaced persons may be forced to leave their homes because of violence, counterinsurgency operations, environmental degradation, development projects, or sudden disasters. Unlike refugees, internally displaced persons remain within national territory, which means that their protection depends primarily on domestic constitutional and administrative frameworks. Yet this also exposes a gap: India does not have a comprehensive statutory regime specifically designed for internally displaced persons (Internal Displacement in India, 2024). As a result, protection is often fragmented, and

displaced populations must rely on a mixture of welfare schemes, ad hoc relief measures, and judicial or administrative intervention. The absence of a dedicated framework makes displacement not only a humanitarian concern but also a governance challenge (India and Internally Displaced Persons (IDPs), 2017).

The relevance of humanitarian law in displacement contexts lies in its normative emphasis on civilian protection, humane treatment, and the mitigation of suffering. International humanitarian law recognizes that displacement is often both a result and a consequence of violence, and that respect for humanitarian norms can reduce forced movement, improve conditions during displacement, and support safe and dignified return (ICRC, 2019). In India, this insight is especially useful for understanding how law should respond when communities are uprooted by violence or emergency measures. A humanitarian perspective requires that the legal system focus not merely on restoring order, but on preserving the minimum conditions of dignity, safety, and agency for displaced persons (Effects of Respect for International Humanitarian Law on Displacement, 2016).

At the same time, humanitarian law in India cannot be understood in isolation from constitutional principles and human rights norms. The Indian legal order places strong emphasis on life, liberty, equality, and dignity, and these values are directly implicated in conflict and displacement settings. Where state action affects civilians in situations of insecurity, humanitarian considerations overlap with obligations of fairness, proportionality, and non-arbitrariness. This is why the Indian context calls for a broader understanding of humanitarian law as part of a larger protection framework rather than as a narrow body of war-time rules (International Humanitarian Law in India: A Critical Case Study, 2013). Such an approach is essential when examining the treatment of persons who are displaced, detained, evacuated, relocated, or otherwise rendered vulnerable by conflict or crisis.

In practical terms, the relevance of this heading for the present study is that it establishes the legal and factual environment in which digital governance

intersects with vulnerability. Conflict, crisis, and displacement are the settings in which data collection becomes most intrusive and least optional, because access to aid, identity, and rehabilitation often depends on the disclosure of personal information. The humanitarian setting therefore magnifies the privacy problem. If legal safeguards are weak, emergency systems may deepen exclusion rather than reduce suffering. For this reason, the study of humanitarian law, conflict, crisis, and displacement in India is indispensable to any serious evaluation of how human dignity can be protected in the digital age (ICRC, 2024).

This section should remain tightly focused on those conditions that make humanitarian protection legally necessary: violence, emergency, forced movement, and vulnerability. Within that frame, India's law must be assessed not only for its formal commitments, but for its ability to secure humane outcomes in the lived reality of people affected by conflict and displacement (How India's Refugee Laws Address Humanitarian Crises?, 2025).

India's Data Protection Framework and Constitutional Privacy Doctrine

India's data protection framework sits at the center of the constitutional right to privacy in contemporary Indian law. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* made it clear that informational privacy is part of the broader guarantee of dignity, liberty, and autonomy under Article 21 (Puttaswamy v. Union of India, 2017). This constitutional foundation has reshaped the way personal data is understood: not merely as information, but as an extension of the person whose control over it must be protected by law (Puttaswamy v. Union of India, 2017).

The Digital Personal Data Protection Act, 2023 is India's first dedicated statute for digital personal data and marks an important shift from fragmented regulation to a more structured legal regime (Digital Personal Data Protection Act, 2023). It creates a framework built around consent, lawful use, rights of the data principal, duties of data fiduciaries, and enforcement through a regulatory board. Within the present heading, its significance

lies in showing how statutory privacy protection now complements constitutional privacy doctrine. The statute does not replace Puttaswamy; rather, it operates within the constitutional mandate that any interference with privacy must satisfy legality, necessity, and proportionality (Digital Personal Data Protection Act, 2023).

At the same time, India's framework remains in a developing phase. The current law establishes basic protections, but questions continue about the strength of individual rights, the scope of state exemptions, and the adequacy of institutional independence in enforcement (Adhithya & Keerthana, 2026). These concerns matter because constitutional privacy is not satisfied by formal recognition alone. A meaningful privacy regime must ensure transparency, accountability, limited processing, and effective remedies when personal data is misused.

Another important dimension of the framework is the relationship between privacy and state power. Indian constitutional doctrine does not treat privacy as absolute, but it requires that state intrusion be justified by a valid law and be proportionate to a legitimate aim. This is especially relevant in digitally mediated governance, where personal data may be collected at scale for welfare delivery, identification, surveillance, or administrative efficiency. In such cases, the danger lies not only in misuse of data, but also in normalizing excessive data collection without adequate safeguards.

For the present study, the relevance of India's data protection framework and constitutional privacy doctrine lies in the normative baseline they provide. Humanitarian settings, crisis response, and displacement management often involve urgent and sensitive data processing. If privacy is constitutionally a matter of dignity, then any legal framework governing such data must be tested against that standard. The combined effect of Puttaswamy and the Digital Personal Data Protection Act, 2023 is therefore to require a more careful, rights-sensitive approach to the handling of personal information in vulnerable contexts (Digital Personal Data Protection Act, 2023; Puttaswamy v. Union of India, 2017).

In short, India's framework is best understood as an evolving dialogue between constitutional principle and statutory regulation. The Constitution supplies the values of dignity and liberty, while the data protection statute supplies the operational rules for digital information governance. The strength of the system will ultimately depend on whether these two layers work together to protect individuals from informational harm while permitting lawful and necessary processing. That balance is the core of privacy law in India within this heading.

Digital Governance, Humanitarian Relief, and Dignity Risks

Digital governance has become central to humanitarian relief in India because emergency assistance is now increasingly mediated through databases, digital identity systems, online registration portals, and automated decision-making tools. In principle, these technologies can improve coordination, reduce duplication, and speed up delivery of aid to displaced or crisis-affected persons. Yet within the present heading, their relevance lies in the fact that efficiency gains are accompanied by serious dignity risks when vulnerable people are required to disclose personal information in conditions of dependence, urgency, and limited choice. The concern is not merely technical; it is deeply legal and normative, because humanitarian relief should protect persons rather than expose them to avoidable harm (ICRC, 2024).

In crisis settings, the collection of personal data often occurs under asymmetric conditions. Individuals affected by conflict, displacement, or disaster may not have the practical freedom to refuse biometric capture, identity verification, or consent-based data sharing if such disclosure is tied to access to food, shelter, compensation, or rehabilitation. This creates a real risk that digital governance becomes coercive in effect, even if it is formally framed as voluntary. The dignity risk here lies in reducing the affected person to a data subject rather than treating them as a rights-bearing individual whose autonomy and security deserve protection (ICRC, 2024).

A further concern is that digital systems used for relief can outlive the immediate emergency and begin serving wider administrative or surveillance

purposes. Data collected for humanitarian assistance may be reused, shared, or retained beyond the original necessity unless strict safeguards are in place. This can produce exclusion, profiling, secondary use, and data breach risks, especially where systems rely on biometric identifiers or interoperable databases. The relevance of this issue to the heading is that humanitarian relief, if poorly governed, may generate informational harm precisely at the moment when the law should be reducing vulnerability (ICRC, 2020).

The legal challenge in India is therefore not to reject digital governance, but to subject it to a dignity-centered framework. In the context of humanitarian relief, that means ensuring necessity, proportionality, purpose limitation, transparency, and accountability in the collection and use of personal data. It also means recognizing that people in crisis are not ordinary data principals in the abstract; they are persons in conditions of dependence whose capacity to consent is often constrained. A rights-sensitive humanitarian approach must therefore evaluate not only whether data processing is lawful, but whether it is humane (Digital Personal Data Protection Act, 2023).

Within this heading, the concept of dignity risk captures the possibility that digital systems may convert humanitarian assistance into an instrument of monitoring, exclusion, or administrative control. Such risks become particularly acute where relief depends on identity verification, data matching, or algorithmic eligibility decisions. If safeguards are weak, the result may be denial of aid, improper profiling, or exposure of sensitive information to third parties. In that sense, digital governance can unintentionally undermine the very humanitarian objectives it is designed to advance (ICRC, 2024).

The significance of this discussion for the present study is therefore confined to one proposition: humanitarian relief in India cannot be assessed solely in terms of speed, scale, or technological sophistication. It must also be assessed in terms of whether the systems used preserve the dignity, privacy, and agency of those they are meant to assist. That is why digital governance and humanitarian relief must be studied together, not as separate policy domains, but as overlapping fields

where the treatment of personal data has direct consequences for human dignity (Puttaswamy v. Union of India, 2017).

Comparative and Normative Analysis

A comparative and normative analysis is essential to this study because it allows the legal framework governing humanitarian data protection in India to be assessed against both external models and internal constitutional values. Within the present heading, the purpose of comparison is not to catalogue foreign laws for their own sake, but to identify principles that can strengthen India's response to humanitarian emergencies while remaining consistent with domestic legal commitments. Comparative inquiry is particularly useful where Indian law is still developing in relation to crisis governance, displacement, and the protection of personal data in vulnerable settings (ICRC, 2024).

From a comparative perspective, international humanitarian data protection practice shows that privacy safeguards are increasingly treated as a core part of humanitarian action rather than as a secondary administrative concern. The ICRC's guidance emphasizes purpose limitation, data minimisation, confidentiality, and risk-based processing as essential standards in humanitarian work. These principles are valuable because they reflect the reality that persons affected by conflict, disaster, or displacement often have little meaningful choice over whether to disclose information. Comparative models therefore highlight the need for a context-sensitive approach rather than a generic privacy template (ICRC, 2020).

Indian law can be compared with these standards to determine whether its present regime is sufficiently tailored to humanitarian vulnerability. The Digital Personal Data Protection Act, 2023 provides an important statutory foundation, but its general structure is designed for digital personal data broadly, not for the unique pressures of relief operations or displacement management (Digital Personal Data Protection Act, 2023). A comparative analysis reveals that humanitarian data protection requires heightened sensitivity to coercive circumstances, urgency-driven consent,

and the risk of exclusion from aid. In this respect, Indian law can benefit from a more explicit legal recognition that data processing in emergencies must be governed by stricter proportionality and accountability norms.

The normative dimension of the analysis is equally important. Normatively, the question is not only what the law permits, but what the law ought to protect in light of constitutional dignity. The Supreme Court's privacy jurisprudence makes clear that personal autonomy and dignity are not separate from informational privacy; they are part of its constitutional foundation (Puttaswamy v. Union of India, 2017). Accordingly, any legal framework that permits large-scale data processing in humanitarian settings must justify itself not merely by administrative efficiency, but by reference to dignity, necessity, and non-arbitrariness. This is especially relevant where people affected by crisis may be compelled to surrender biometric, identity, or location data in order to receive basic assistance.

A normative analysis also requires asking whether humanitarian relief systems in India preserve the agency of vulnerable persons or quietly transform them into objects of surveillance. If digital governance is used without clear safeguards, it may produce exclusion, misuse, and long-term informational harm. By contrast, a dignity-based framework would insist that humanitarian data systems be limited to legitimate relief purposes, subject to oversight, and designed to minimise intrusion (ICRC, 2024). Such a framework would not oppose digital governance, but would insist that technological efficiency never override the moral and constitutional obligation to respect human dignity.

Within the scope of this heading, comparative and normative analysis therefore serves two connected functions. First, it identifies better practice standards from humanitarian data governance and privacy law. Second, it translates those standards into evaluative criteria for India, grounded in constitutional values and the lived realities of crisis-affected persons. The result is a more principled basis for reform, one that enables India to align humanitarian relief with dignity, legality, and rights protection in the digital age.

Conclusion and Suggestions

The analysis undertaken in this study demonstrates that the intersection of humanitarian law, digital governance, and data protection in India must ultimately be judged through the lens of human dignity. Humanitarian action in conflict, crisis, and displacement settings is intended to protect life, security, and survival, yet the growing reliance on digital systems has created new forms of vulnerability. The ICRC has expressly stated that protecting personal data is integral to protecting the life, integrity, and dignity of individuals in humanitarian contexts. This proposition is particularly relevant in India, where digital governance increasingly mediates access to identity, welfare, and emergency assistance.

The principal conclusion that emerges is that India's legal framework contains important normative foundations, but it remains insufficiently tailored to the realities of humanitarian data processing. On the one hand, the constitutional recognition of privacy in *Justice K.S. Puttaswamy (Retd.) v. Union of India* establishes that privacy is an aspect of dignity, autonomy, and personal liberty under Article 21. On the other hand, the Digital Personal Data Protection Act, 2023 provides a statutory structure for digital personal data processing that acknowledges both individual rights and lawful state or institutional use. Together, these developments mark a significant evolution in Indian privacy law. Yet neither constitutional doctrine nor the general statutory framework fully addresses the distinct coercive pressures, dependency conditions, and informational asymmetries that characterize humanitarian emergencies.

A further conclusion is that digital systems used in relief and rehabilitation cannot be assessed merely by reference to administrative efficiency. A technologically efficient system may still be legally and ethically deficient if it compels disclosure without meaningful choice, retains data beyond necessity, enables secondary use, or exposes affected persons to profiling and exclusion. In humanitarian contexts, the issue is not only whether data is processed lawfully, but whether it is processed humanely. A dignity-based approach therefore requires closer attention to

necessity, proportionality, purpose limitation, and contextual vulnerability.

Several recommendations follow from this conclusion. First, India should develop humanitarian-specific data governance standards, either through statutory amendment, delegated rules, or formal policy guidance, to regulate the processing of personal data during conflict, disaster response, displacement management, and emergency relief. Such standards should recognize that persons in crisis are not ordinary data subjects and therefore require heightened protection. Second, the legal framework should impose stricter duties regarding data minimisation, retention limits, transparency, and independent oversight wherever aid delivery depends on digital systems or biometric verification.

Third, humanitarian data practices in India should be anchored in the constitutional principles articulated in *Puttaswamy*, especially legality, legitimate state aim, and proportionality. These principles should function not only as judicial standards of review but as operational standards for administrators, humanitarian actors, and public authorities. Fourth, relief architecture should incorporate safeguards against exclusion, including alternative mechanisms for receiving assistance where individuals cannot comply with digital or biometric requirements. This is necessary to ensure that technological systems do not deny aid to those whom humanitarian relief is designed to protect.

Finally, a broader normative recommendation is that Indian law should explicitly recognize informational dignity as part of humanitarian protection. Personal data in crisis settings is not merely an administrative input; it is deeply connected to identity, autonomy, and security. Any future development of India's humanitarian and data protection framework should therefore proceed from the premise that relief must not become a vehicle for surveillance or control. Rather, digital governance in humanitarian contexts must remain subordinate to the constitutional commitment to dignity and the humanitarian imperative of protection.

In sum, the study concludes that India possesses the beginnings of a robust legal response, but not yet a fully adequate one. The path forward lies in integrating humanitarian sensitivity with constitutional privacy doctrine and statutory data protection. Only then can India ensure that the digital management of crisis remains consistent with the fundamental value that underlies both humanitarian law and privacy law alike: the protection of human dignity.

References

- Adhithya, G. M., & Keerthana, K. (2026). Data privacy and protection in India: A critical doctrinal analysis of the Digital Personal Data Protection Act, 2023 in the light of constitutional standards and international benchmarks. *Indian Journal of Legal Review*, 6(7), 13.
- Analysing international humanitarian law in the Indian context. (2023, November 22). KSLR. <https://www.kljp.org/articles/article-analysing-international-humanitarian-law-in-the-indian-context>
- Bibhu, N. K., & Dubey, B. (n.d.). Implementation of Consumer Protection Act 2019: A study of the role of consumers. *Bihar Journal of Public Administration*, 439. https://www.researchgate.net/profile/Nishi-Kant-Bibhu/publication/410511119_IMPLEMENTATION_OF_CONSUMER_PROTECTION_ACT_2019_A_STUDY_OF_THE_ROLE_OF_CONSUMERS
- Digital Personal Data Protection Act, 2023, India Code. https://www.indiacode.nic.in/handle/123456789/22037?view_type=browse
- Effects of respect for international humanitarian law on displacement. (2016, October 1). GSDRC. <https://www.gsdr.org/wp-content/uploads/2016/10/HDQ1393.pdf>
- How India's refugee laws address humanitarian crises? (2025, May 9). Lloyd Law College Blog. <https://www.lloydlawcollege.edu.in/blog/india-refugee-laws-humanitarian-crises.html>
- India and internally displaced persons (IDPs). (2017, November 5). Live Law. <https://www.livelaw.in/india-internally-displaced-persons-idps>
- India's engagement with international humanitarian law: A law and policy analysis. (2024, January 12). SSRN. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4802116_code6352235.pdf
- Internal displacement in India: Causes, protection and dilemmas. (2024, August 26). Forced Migration Review. <https://www.fmreview.org/lama/>
- International Committee of the Red Cross. (2019, April 7). How international humanitarian law protects in war and why it matters. <https://www.icrc.org/en/document/ihl-displacement>
- International Committee of the Red Cross. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, 102(913), 1.
- International Committee of the Red Cross. (2024). Handbook on data protection in humanitarian action. <https://www.icrc.org/en/data-protection-humanitarian-action-handbook>
- International humanitarian law in India: A critical case study. (2013). KSLR. <https://kslreview.org/index.php/kslr/article/view/998>
- Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.