BEYOND DELETION: THE RIGHT AGAINST ALGORITHMIC REDISCOVERY AND THE CONSTITUTIONAL BALANCE BETWEEN PRIVACY AND FREE SPEECH IN INDIA

Aadrika Prakash Gupta, OP Jindal Global University

ABSTRACT

The constitutional issue presented by "digital permanence" does not simply involve the potential for information to remain available online. Instead, the problem lies in the fact that outdated, replaced, or irrelevant information may become searchable and amplified via algorithms. In this paper I will consider whether Indian Constitutional Law provides a limited "Right Against Algorithmic Re-Discovery" under the existing guarantees of Privacy, Dignity, Autonomy, and Freedom of Speech. I argue that the relevant constitutional inquiry should not be whether an individual has an unfettered right to delete his/her past, but rather whether the persistent algorithmic prominence of legally obtained information, under certain conditions, places an undue burden on the individual's privacy. Article 19(1)(a) of the Constitution of India mandates the courts to safeguard these rights; however, the task of achieving a structure of proportionality must guide the process[1]. Drawing upon recent judgments of the Delhi High Court, I suggest that a Court of Law may be guided by the distinction between preserving and deleting information, as well as the difference between making information discoverable through searching and increasing its visibility through algorithmic amplification. A structured definition of balancing is needed to guide the Court when determining whether preservation, deletion or masking is appropriate for preserving information and providing protection against algorithmic amplification.

[1] *K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India); Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).*

Introduction

The jurisprudential frameworks for privacy were developed at a time when there were physical barriers to obtaining data. Even though organizations such as media outlets, courts, and archives created documents, they had to spend money, time, and effort to obtain those documents. Today's technologies have changed how quickly we can access data. Digital tools today allow people to quickly find old news stories from many years ago. Judicial documents from earlier times may be among the first search results for certain topics.

Additionally, algorithmic recommendation systems can bring attention to less-known or less-central historical records through association with a person's current digital identity. These changes create a constitutional issue that is beyond what has been considered part of the "right to be forgotten." The right to be forgotten generally refers to removing or de-indexing information that is no longer necessary or relevant[2]. However, the focus here is a different type of phenomenon: algorithmic rediscovery. When automated systems (e.g., search engines, ranking protocols) continuously highlight technically obtainable data by associating it with a person's current digital identity, this phenomenon occurs.

Thus, the real problem is not the continued availability of data, but its continuous exposure. Differentiating between these two types of privacy issues has significant implications for constitutional law. When a publisher is forced to remove an accurate historical account, it directly conflicts with Article 19(1)(a). Instructing a search engine to lower the ranking of an outdated article in named-based searches does not eliminate the original source. While complete removal of information would undermine the integrity of historical archives, limiting the ability to find information only limits how easily existing records can be found[3].

Therefore, it will be important to distinguish between these two legal frameworks when developing a rational Indian jurisprudence. The present research is particularly timely given the Supreme Court's definitive ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India, which recognized that privacy is a fundamental right guaranteed under Article 21 of the

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, art. 17; *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014).
[3] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD),* Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014).

Constitution[4]. Puttaswamy created the philosophical framework for a right to privacy based on human dignity, autonomy, liberty, and self-determination with respect to personal information[5]. However, Puttawamy did not establish an absolute right to regulate all aspects of an individual's personal data.

Furthermore, Puttawamy did not settle the conflict between informational privacy and the competing interests of freedom of expression and the public's right to access factual information. Recent developments in Indian law suggest that these conflicts are no longer merely academic. On May 25, 2026, the Delhi High Court ruled in Laksh Vir Singh Yadav v. Union of India that the right to be forgotten falls under Article 21's protection of privacy. The Court ordered search engines to de-index certain judicial documents from search results based on names, but allowed access to the original judgments via citation or case number[6]. The Laksh Vir Singh Yadav ruling represents a move away from the simple dichotomy of either existing online completely or disappearing entirely from view. The Court's ruling suggests that while data may be stored in archives, the way search engines make that data available to their users is subject to constitutional review[7]. This article posits that Indian constitutional doctrine should create a limited right to protect against algorithmic rediscovery. This right will allow individuals to protect themselves from the ongoing and excessive promotion by algorithms of personal data which no longer possesses any relevance. The right will apply where continued exposure causes substantial damage to an individual's dignity without serving a legitimate public interest, and will typically lead to remedies such as de-indexing or contextual masking rather than complete removal of the data.

Moving From The "Right To Be Forgotten" To Algorithmic Rediscovery

In most cases, the conceptual foundation for the right to be forgotten comes from the European Court of Justice's decision in google spain sl v. Agencia Española de Protección de Datos[8]. The Court stated in Google Spain that under specific circumstances, individuals could request that search engines delete links to their personal information from search results. The Court made it clear that it did not give permission to destroy history; however, it distinguished between data that continues to exist on a primary source website and data that is available through name-

[4] *K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).*
[5] *ibid.*
[6] *Laksh Vir Singh Yadav v. Union of India, W.P. (C) No. 1021 of 2016 & connected matters (Delhi High Court May 29, 2026) (India) (2026:DHC:4891).*
[7] *ibid.*
[8] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD),* Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014).

based searching[9]. This distinction is vital for India's constitutional framework, because maintaining historical accuracy, judicial transparency, and democratic accountability are all dependent upon keeping official records intact.

However, keeping official records intact does not imply that every person whose name appears in the records must remain searchable through those records forever. An official judgment may continue to exist in the public record while still allowing individuals to find the underlying judgment via some means other than their names. While Indian legal literature has traditionally called a "right to be forgotten," this term may cause confusion. To "forget" means to completely erase data, whereas "algorithmic rediscovery" refers to how ranking and recommendation systems transform previously hidden data into newly visible data. For instance, even if a person was arrested and later cleared of all charges, the original arrest record will remain a historical fact.

However, when an algorithmic search engine gives more weight to a person's arrest record than to his/her/their subsequent acquittal of those charges, the person suffers a constitutional injury. The injury arises from the fact that an individual's arrest record exists, however, from a technical design that gives more weight to one piece of history than to its ultimate resolution. Therefore, these issues can be divided into three phases: preservation, discoverability, and amplification. Preservation deals with the archival storage of data; discoverability relates to an individual's capacity to discover data via traditional search mechanisms; and amplification pertains to the methodical prioritization or promotion of that data. The constitutional argument presented here only pertains to the last two categories.

Moreover, this nuanced approach addresses the main criticism directed towards the right to be forgotten – that it serves as a mechanism to suppress uncomfortable truths. Generally speaking, a right against algorithmic rediscovery does not eliminate primary sources of data. Instead, it determines whether continuing prominence of a specific record is justified given the individual's present situation and the overall public interest.

Constitutional Foundations: Articles 21 And 19(1)(a)

A. Article 21, Privacy, Dignity and Informational Autonomy

The first element of this paper is the case Puttaswamy. In Puttaswamy, the nine-judge

[9] *ibid.*

Constitutional Bench definitively found that Article 21 guarantees an individual's right to privacy as a fundamental right[10]. Not only did Puttaswamy consider the physical separation of an individual from other people, but it also considered the decisional autonomy, dignity, and control over their own information. The Court's understanding of informational privacy is particularly relevant in terms of algorithmic "rediscovery" of information about an individual, given that an individual's personal information can hinder their ability to develop relationships with other individuals[11].

In addition, the Court's understanding of informational privacy has constitutional relevance irrespective of whether information is confidential or non-confidential. Availability of public information does not automatically mean that an individual's privacy cannot be negatively impacted by such information[12]. Informational privacy will have constitutional implications when the continuous collection, accessibility, and dissemination of personal information hinders an individual's capacity to exercise autonomy. The rationale supporting this position is also reinforced by the decision in Navtej Singh Johar v. Union of India, which established that privacy and dignity are both integral aspects of an individual's identity and autonomy[13]. For the purposes of answering this question, Navtej Singh Johar is important not for its discussion of homosexual rights (the specific subject matter of the case), but for how it understood constitutional dignity. Constitutional dignity protects individuals not only from direct physical interference with their person, but also from the various legal and social barriers that inhibit them from acting as autonomous individuals[14].

In summary, therefore, the reasoning utilized in Article 21 supports the argument that an individual should not be constitutionally obligated to continually experience digital exposure simply because information regarding them was at one time publicly available. There are however limitations to this argument. An individual does not possess a constitutional right to control what constitutes reality. Whether information is embarrassing, detrimental to one's reputation, or simply unwanted does not automatically render its publication unconstitutional.

Therefore, Puttaswamy's proportionality test is essential. An intrusion upon an individual's right to privacy must stem from a valid law, be for a valid purpose, and be proportionally related

[10] *K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).*
[11] *ibid.*
[12] *ibid.*
[13] *Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (India).*
[14] *ibid.*

to achieving that objective[15]. Puttaswamy's framework creates the constitutional accountability required to differentiate between valid claims for privacy protection and efforts to suppress undesirable information.

B. Article 19(1)(a) and the Public Value of Information in Democracies

As discussed above, the right to freedom of speech and expression is not limited to the rights of a speaker to produce information. In a democracy, an informed citizenry depends upon the ability to produce and consume information[16].

Therefore, if citizens were able to consistently request that their information be removed from public access, the processes of journalism, history writing, academic research and public accountability would be greatly affected. As demonstrated in Shreya Singhal v. Union of India, when regulating online information, the Courts must exercise judicial restraint and prudence[17]. In Shreya Singhal, the Supreme Court struck down Section 66A of the Information Technology Act 2000 as being unconstitutional because of its broad and vague language that provided for undue restriction on protected speech[18]. Shreya Singhal demonstrates that restrictions on digital speech cannot be based on uncertain standards that allow for arbitrary enforcement. This is particularly relevant to algorithmic rediscovery. If a vague constitutional standard allows for removal of information when it is "harmful," "embarrassing," or "outdated," then there will be uncertainty about what information may lead to legal action, which will create a chilling effect.

Therefore, the answer is not to choose between Article 21 and Article 19(1)(a), but rather to recognize that both rights can coexist. The constitutional issue is not whether privacy or speech "wins." Instead, the issue is whether a particular type of digital distribution is proportional to the public interest served by continued accessibility.

Emerging Indian Jurisprudence

Over recent years, Indian courts have placed an increasing emphasis on the right to be forgotten under Article 21. Prior to these cases, courts such as those in R. Rajagopal v. State of Tamil Nadu had already recognized privacy as an inherent right under Article 21's right to life and

[15] *K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).*
[16] *Secretary, Ministry of Information & Broadcasting v. Cricket Ass'n of Bengal, (1995) 2 SCC 161 (India).*
[17] *Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).*
[18] *ibid.*

personal liberty, and at the same time acknowledged the right of the press to report on matters that enter the public domain[19].

Therefore, R. Rajagopal had previously identified the fundamental conflict between privacy and free expression; they are not mutually exclusive constitutional rights. Recent developments are more direct. In Jorawer Singh Mundy v. Union of India, the Delhi High Court examined the implications of continued online accessibility of a judgment concerning an individual who had been acquitted[20]. Jorawer Singh Mundy illustrated the practical problems arising from an individual's name remaining permanently linked to an allegation even after the judicial resolution of that allegation is positive for that individual[21]. Jorawer Singh Mundy represents an initial judicial attempt to differentiate open justice from unlimited digital discoverability. A significant development occurred in Laksh Vir Singh Yadav v. Union of India, decided on May 29, 2026. The Delhi High Court considered the right to be forgotten as an element of informational privacy under Article 21, and established a system for digital judicial records. Significantly, the court did not merely direct the destruction of judicial documents[22]. Rather, the court ordered search engines to delist specific content from name-based searches, and directed Indian Kanoon to limit name-based search capabilities while providing access to judgments via case number, citation, court information and date[23]. The remedial framework developed by the court has constitutional significance. It recognizes that open justice does not necessarily require maximum name-based discoverability[24]. While a judgment continues to form part of the public legal record, its algorithmic association with a private individual's name may be restricted under specific circumstances

Furthermore, the subsequent September 2026 order in the same case is also noteworthy as it was observed by the Delhi High Court that the Union Government intended to abide by the May 2026 order[25]. However, this order should be interpreted cautiously. Laksh Vir Singh Yadav is a High Court judgment and not a Supreme Court constitutional bench decision and therefore may undergo further modification during future litigation. Therefore, Laksh Vir

[19] *R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (India).*
[20] *Jorawar Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306 (India).*
[21] *ibid.*
[22] *Laksh Vir Singh Yadav v. Union of India, W.P. (C) No. 1021 of 2016 & connected matters (Delhi High Court May 29, 2026) (India) (2026:DHC:4891).*
[23] *ibid.*
[24] *ibid.*
[25] *Laksh Vir Singh Yadav v. Union of India, W.P. (C) No. 1021 of 2016 & connected matters (Delhi High Court May 29, 2026) (India) (2026:DHC:4891).*

Singh Yadav provides a fundamental jurisprudential basis for the proposed right and not an absolute national constitutional rule.

Additionally, the statutory landscape needs to be taken into account. The Digital Personal Data Protection Act 2023 grants rights regarding rectification and erasure of personal data and provides a broader statutory framework for data governance[26]. Digital Personal Data Protection Rules 2025 were subsequently notified with staggered commencement[27]. However, data protection legislation should not be viewed as automatically resolving the constitutional dilemma. Constitutional privacy exists at a higher normative plane than ordinary statutory privacy, particularly when informational control conflicts with expression, open justice and public access to information.

The Constitutional Problem of Algorithmic Amplification

The main problem with algorithmic rediscovery is that algorithms do not simply reproduce information; they decide what information can be seen. For example, if you find a story from 2008 about someone who has never been involved in another controversy since then, you could probably find the same exact wording in a search result for that person's name as well. However, those two results would have very different social effects.

As a result, the old distinction between "publication" and "non-publication" is becoming less effective. Algorithms provide an intermediate area of law in which information exists in technical availability but provides too much visibility. In particular, the problem is most apparent when there is missing information behind the information being made available. Suppose someone was accused of a crime in 2010, found innocent in 2012, and then lived a life free of controversy. A search engine that continually displays the 2010 accusation before the acquittal does not necessarily display false information.

However, the overall display of information can create a misleading impression. Therefore, constitutional protection of privacy should provide a way to address misleading displays of contextually relevant information without having to deem the original display of information unlawful. This is where the concept of dignity comes into play. The constitutional harm may

[26] Digital Personal Data Protection Act, No. 22 of 2023, §§ 8, 12–13 (India).
[27] Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India (2025) (India).

be ongoing rather than immediate. Someone may not see one specific instance of publication that violates article 21. Instead, he or she may suffer negative consequences resulting from years of consistent technological association of his/her identity with a dead event including loss of job opportunities, decreased ability to form relationships, diminished participation in social events, and lessened psychological independence[28].

Thus, the constitutional harm is relational: information becomes harmful due to its consistency in technology with the individual. Nonetheless, acknowledging that there is harm does not warrant judicial regulation of the Internet without limit. A constitutional doctrine must differentiate between legitimate rediscovery and illegitimate amplification. Generally speaking, information regarding corruption by a government employee, significant criminal activity, major political events, professional wrongdoing, or currently topical issues will provide a basis for a strong public interest rationale[29].

Towards A Proportionality-Based Right Against Rediscovery

The best constitutional method is to think of the right to algorithmic rediscovery as a qualified derivative of informational privacy rather than an independent absolute right. Initially, the inquiry should focus on the nature and status of the claimant. Generally, the privacy rights of an average private individual will be more protected than those of a public official whose activities involve the exercise of public authority. Nonetheless, public figures cannot be entirely excluded from the protections afforded by privacy. The appropriate inquiry should continue to assess whether the information has a substantial connection to a valid public interest[30].

Secondly, courts should evaluate the nature of the information. False, outdated, incomplete, or materially misleading information due to subsequent developments provides a stronger basis for intervention than information that continues to accurately describe current events

Thirdly, courts should evaluate temporal relevance. Although time cannot automatically result in the termination of free speech, the passage of time may affect the balance between privacy and public interest. A decade-old private dispute conclusively resolved represents a

[28] *K.S. Puttaswamy, (2017) 10 SCC 1 (India); Navtej Singh Johar, (2018) 10 SCC 1 (India).*
[29] *R. Rajagopal, (1994) 6 SCC 632 (India); Secretary, Ministry of Information & Broadcasting, (1995) 2 SCC 161 (India).*
[30] *K.S. Puttaswamy, (2017) 10 SCC 1 (India)*

constitutionally different situation than ongoing evidence of public corruption. Fourthly, courts should assess the degree of algorithmic amplification. The fact that information can theoretically be located somewhere online should not automatically lead to intervention. The more important question is whether technological systems have transformed previously obscure historical material into a sustained and visible part of an individual's digital identity.

Lastly, courts should determine whether alternative remedies exist that are less restrictive. This is where proportionality, specifically the least restrictive means test, is essential. Anuradha Bhasin v. Union of India reaffirmed the constitutional requirement that restrictions placed on fundamental rights cannot exceed what is necessary to achieve the legitimate objective[31]. Applied here, deletion should typically be used as a last resort. De-indexing is generally less restrictive because the original source material remains accessible. Contextualization may be even less intrusive: a search result pertaining to an old criminal accusation could be accompanied or linked with the subsequent acquittal. Masking names in a judicial database can protect an individual's identity while maintaining a judgment's precedential and historical value. These remedies preserve much of the informational value protected by Article 19(1)(a) while reducing the privacy harm protected by Article 21. Laksh Vir Singh Yadav's method is therefore particularly commendable. Laksh Vir Singh Yadav's argument that judgments remain accessible via case numbers, citations, court details, and dates indicates that privacy and open justice need not be seen as two mutually exclusive alternatives[32]. Rather than regulating access to information in a binary manner, constitutional adjudication may regulate the methods by which information becomes available.

Objections and Constitutional Safeguards

Perhaps the greatest objection to a right against algorithmic rediscovery is that such a right would create a “constitutional” memory hole. There exists the possibility that influential persons could use their privacy rights to suppress damaging yet factually correct reporting.

Additionally, there exists the possibility that government agencies could use their privacy rights to avoid being subject to governmental scrutiny of public officials. Further, there exists the possibility that courts could become the final arbiters of historical fact as opposed to protectors

[31] *Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).*
[32] *Laksh Vir Singh Yadav v. Union of India, W.P. (C) No. 1021 of 2016 & connected matters (Delhi High Court May 29, 2026) (India) (2026:DHC:4891).*

of constitutional rights. Such objections are reasonable and warrant a limited doctrine. However, the solution is not to deny the existence of a right against algorithmic rediscovery; rather, the solution is to establish specific limits.

Specifically, journalism in the public interest should be afforded a high degree of protection. Information pertaining to corruption, public office, serious criminal behavior, public health problems, institutional wrongdoing, and significant democratic interests should typically be readily available[33]. Claimants should be required to demonstrate substantial and extreme harm resulting from the publication of information about them and not merely allege embarrassment. A second objection relates to intermediary burdens. Search engines may argue that determining whether to remove content based upon a claimant's right to privacy transforms private corporations into quasi-judicial entities. This is also a legitimate concern.

Therefore, a constitutional framework should establish judicial or independent adjudicatory determinations as the preferred method for resolving disputes regarding content removal as opposed to establishing broad proactive monitoring requirements for intermediaries. A third objection relates to whether algorithmic ranking itself constitutes expression. Under Article 19(1)(a)'s expansive interpretation, the state should exercise caution in dictating what information a private platform must display[34]. Once again, the response should be based upon proportionality. The proposed doctrine should not generally compel platforms to remove viewpoints simply because the government disagrees with those viewpoints. Instead, the focus should be on specific claimant-specific interventions based upon evidence-based privacy harm and subject to due process protections.

Finally, the doctrine must recognize the technological limitations associated with deleting digital information. Digital information can be copied, stored, replicated, archived, republished, etc.

Therefore, a constitutional remedy should attempt to achieve realistic goals. The goal is not to eliminate history; however, the goal is to prevent publicly available information from becoming an involuntary and algorithmically-enforced identity marker.

[33] *R. Rajagopal, (1994) 6 SCC 632 (India)*
[34] *Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India); Secretary, Ministry of Information & Broadcasting v. Cricket Ass'n of Bengal, (1995) 2 SCC 161 (India).*

Conclusion

The Constitutional Issue of the Digital Age is not that the Internet has the ability to remember, but rather that the Internet has the ability to remember both selectively and persistently and also in a manner determined by algorithms. The individual may have moved beyond the event in question in terms of the law and yet the search engine will still display the event as a key feature of the person's identity. There exist various tools within Indian Constitutional Law which can deal with this issue. The right to privacy and dignity as well as the right to informational autonomy is protected under Article 21, as established through Puttaswamy[35]. Article 19(1)(a) provides protection for the dissemination of information and prevents overly broad restrictions on freedom of expression. This article has been reinforced through Shreya Singhal[36] and other case law. Maneka Gandhi provides the overall constitutional commitment to fairness and reasonableness in regards to restrictions placed upon the exercise of individual liberty[37]. The proportionality requirement for restrictions on individual liberty was further reinforced through Anuradha Bhasin[38]. Navtej Singh Johar reaffirmed the importance of dignity and autonomy in relation to an individual's status as a 'constitutional person'[39]. Most importantly, Laksh Vir Singh Yadav illustrated how Indian Courts are beginning to distinguish between preserving publicly available information and unrestricted digital availability.[40]

Therefore, the best constitutional position regarding the Internet's memory would be neither an absolute right to be forgotten nor an absolute right for the Internet to remember. Instead, the best constitutional position is a right to protection from disproportionately excessive rediscovery via algorithms. A right such as this would not destroy history; instead, it would establish rules concerning the circumstances under which historic information continues to be transformed into present identity. Ordinarily, the most appropriate constitutional remedy would be proportional. The remedies include retaining underlying documentation, limiting excessive discoverability, removing entries from name-based searches, contextualising incomplete information, and where necessary, concealing. Deletion would ordinarily be considered a last

[35] *K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).*
[36] *Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India)*
[37] *Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).*
[38] *Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).*
[39] *Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (India).*
[40] *Laksh Vir Singh Yadav v. Union of India, W.P. (C) No. 1021 of 2016 & connected matters (Delhi High Court May 29, 2026) (India) (2026:DHC:4891).*

resort[41].

Ultimately, one must determine whether continued algorithmic recognition serves a sufficiently strong public interest to justify continued intrusion into the individual's right to informational privacy. This approach recognises India's Constitution's fundamental structure. It views privacy not as a means to suppress truth and free speech not as a means to allow unlimited exposure. Rather, this approach acknowledges that constitutional liberty sometimes requires society to recollect responsibly. Within the digital constitutional order, the question is no longer simply whether an individual has a right to control what is said about him or her. The question is now whether society's method of recalling him or her has become excessive.

[41] *Laksh Vir Singh Yadav v. Union of India, 2026 SCC OnLine Del 4891; Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).*