THE RIGHT TO BE FORGOTTEN OF VICTIMS IN INDIA: SPECIAL EMPHASIS ON SEXUAL ABUSE AND THE BALANCE BETWEEN VICTIM PRIVACY, DIGNITY AND THE PUBLIC RIGHT TO KNOW

Amina Fayaz Shejwalkar*

ABSTRACT

The right to be forgotten has become a pressing concern in the digital age, especially for sexual-offence survivors, whose personal information can remain online long after it was first published. Unauthorised disclosure of a survivor's identity harms their privacy, dignity and social life, and can lead to harassment and secondary victimisation. This article examines the right to be forgotten in India, with special emphasis on sexual-abuse survivors, and weighs it against freedom of expression, open justice and the public's right to know.

It analyses privacy under Article 21, relevant judicial decisions and statutory provisions restricting disclosure of victims' identities. It also considers how platforms, publishers and search engines keep identifying information in circulation, and compares the position in the European Union and the United Kingdom. The analysis finds gaps in India's framework, mainly in obtaining timely removal, preventing repeated disclosure and enforcing court directions across platforms.

The article argues for clear procedures for redaction, removal and de-indexing, time-bound compliance with court orders, stronger platform accountability and accessible remedies. These measures must remain proportionate and preserve legitimate public access to legal information. A balanced and practical framework can protect survivors' privacy and dignity without needlessly restricting expression or open justice.

Keywords: Right to be Forgotten, Informational Privacy, Open Justice, Data Protection.

*BA LLB, SECOND YEAR, RIZVI LAW COLLEGE, MUMBAI.

INTRODUCTION

Victims of sexual offences are exposed to publicity once the criminal proceedings have concluded. In the digital age, once information is published on the internet, it is very hard to control the spread. This means that the personal details of the victim could remain visible online, and they may feel exposed to unnecessary publicity[1]. Once the personal details of the victim of sexual offence are made known, there will be three issues:

These issues arise because it becomes clear that there are limitations to protecting victims of sexual offences from being exposed. How can we prevent these issues and protect individuals from remaining identifiable online? This is where the right to be forgotten comes into play with regard to the issues of erasure, limitation and de-indexing[2]. However, this is not an absolute right and needs to be balanced with the right of the public to know.

The right to be forgotten (RTBF) is tied closely to the right to privacy, which is a fundamental right within the Indian Constitution[3]. However, it does have limitations and does not guarantee complete erasure from the public. This should be balanced with the right to free speech and expression under Art. 19(1)(a).[4]

The Supreme Court's decision in Nipun Saxena v. The Union of India explains that the prohibition of disclosure should not just stop at the name of the party but extend to any information that could expose the individual[5]. Recently, the Delhi High Court has had an important case of Laksh Vir Singh Yadav v. The Union of India[6]. Here, the victim had their name and personal details published on an online database. The court here has given clear guidelines on how to de-index to prevent searches using their name and gave other preventative measures to safeguard[7] them. The Supreme Court shows how important it is to differentiate between keeping records of the judiciary and preventing name searches.

[1] Nipun Saxena v Union of India (2019) 2 SCC 703; Bharatiya Nyaya Sanhita 2023, s 72.
[2] Laksh Vir Singh Yadav v Union of India (Delhi High Court, W.P.(C) 1021/2016 and connected matters, 29 May 2026) [188]–[191].
[3] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[4] Constitution of India 1950, art 19(1)(a).
[5] Nipun Saxena v Union of India (2019) 2 SCC 703.
[6] Laksh Vir Singh Yadav v Union of India (Delhi High Court, W.P.(C) 1021/2016 and connected matters, 29 May 2026).
[7] Laksh Vir Singh Yadav v Union of India (Delhi High Court, W.P.(C) 1021/2016 and connected matters, 29 May 2026) [188]–[191], [211]–[217].

This article will look at whether the current legal framework in India provides sufficient protection to victims of sexual offences from exposure online. I will analyse the constitutional principles, statutory provisions, case law and the limitations to remedies. I will also look at the conflicting issues of victim privacy, dignity and the right to free speech. My main argument is that there is no need to completely erase the judiciary records to protect the victim. Instead, in the correct circumstances, you can obscure personal details and limit name searches to provide a more balanced approach[8]. This will ensure that the legal value of the decision is maintained whilst also protecting the victim. This article will look at the current limitation to the right to be forgotten and how improvements can be made without affecting the right to information of citizens.

CONCEPT AND LEGAL FRAMEWORK OF THE RIGHT TO BE FORGOTTEN IN INDIA

The right to be forgotten (RTBF) refers to the person's right to seek to remove the availability of the person's information online or limit how easily it is accessible in the digital world, where its continued availability is no longer required, justified or causes disproportionate harm[9]. The concern arises from the way information is used or behaves in the digital space. Where a printed report is difficult to access or locate years later, online material does not face the same issue. It can stay accessible indefinitely, be copied and transferred across several platforms and appear easily in search engines long after the circumstances of its publication have changed. Without deindexing, it can appear easily and resurface with just a name search of the victim.

The RTBF responds to such problems where permanent accessibility may harm privacy and dignity, affecting the victim's ability to move beyond their past. Therefore, the RTBF addresses the relation between this everlasting accessibility and the personal interest of the victim, their privacy, dignity and control over their personal information[10].

Article 21 of the Constitution of India states that no person shall be deprived of life or personal liberty except according to procedure established by law[11]. Throughout history, the Supreme

[8] Justice K S Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1; Laksh Vir Singh Yadav v. Union of India (Delhi High Court,W.P.(C) 1021/2016 and connected matter,29 May 2026) [188]-[191]
[9] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (opinion of Sanjay Kishan Kaul J); Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) EU:C:2014:317.
[10] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026).
[11] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

Court has interpreted this protection broadly. In Puttaswamy, a nine-judge Bench held that privacy is a fundamental right protected by the Constitution[12]. Privacy includes not only the ability to make important personal choices but also to exercise control over personal information.

Privacy and personal information are particularly relevant to online publication. Personal information can reveal intimate details about a person's life, relationships, family, work and other experiences. When such information is made widely accessible without sufficient justification, the person may lose control over how it is circulated and used. The digital environment can increase this harm because information can be searched, copied and shared repeatedly across platforms.

Dignity, being closely connected to privacy, comes under Art. 21[13]. Art. 21 protects more than physical existence. It moreover supports a person's ability to live with dignity. For a victim of sexual abuse, public identification may disturb their lives and result in humiliation, blame, social exclusion or unwanted questioning and attention. These consequences don't die with the verdict but can continue long after the criminal proceedings have ended. Protecting identity can help the victim participate in legal proceedings without facing further harm to their image.

However, keeping in mind, Article 21 does not automatically require the removal of every reference to a person's past. Privacy must be balanced against other constitutional interests, including freedom of speech and expression under Article 19(1)(a)[14]. The balance depends on the circumstances. Information about a victim's identity is different from information about the conduct of public officials or the reasoning of a court.

Therefore, the right to privacy should be understood as a basis for meaningful protection when required, and not as a general power to erase public records. Where the law expressly prohibits disclosure of a sexual-abuse survivor's identity, the question is not simply whether the information is embarrassing or humiliating. The relevant issue is whether the disclosure violates a legal duty to protect the victim and their daily life[15].

[12] Constitution of India 1950, art 21; Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[13] Constitution of India 1950, art 21.
[14] Constitution of India 1950, arts 19(1)(a) and 21.
[15] Nipun Saxena v Union of India (2019) 2 SCC 703; Bharatiya Nyaya Sanhita 2023, s 72.

Several judicial case decisions help in understanding the relationship between privacy, dignity and the right to be forgotten.

In Justice K.S. Puttaswamy (Retd.) vs Union of India, the Supreme Court recognised privacy as a fundamental right and also discussed the importance of informational autonomy. Justice Kaul's opinion considered the right to be forgotten, while also making clear that it could not be absolute. This decision provides a constitutional backing for claims involving the continued online circulation of personal information[16].

In Nipun Saxena v. Union of India, the Supreme Court considered the protection of a sexual-offence victim's identity. It held that the prohibition on disclosure extends to information that may directly as well as indirectly identify a victim; this includes the age, family, workplace, hometown and other identifiers of the victim. The judgment also issued directions concerning the handling and publication of information in sexual-offence cases. It is particularly important because it establishes that victim anonymity is not merely a matter of personal preference but a matter of grave importance[17].

Even in R Rajagopal v State of Tamil Nadu, the Supreme Court examined privacy in the context of publication of information. The decision recognised limits on the publication of private matters at the same time it considered the freedom of the press. It illustrates the need to distinguish legitimate public reporting from unnecessary interference with private life[18].

More recently, the Delhi High Court considered the right to be forgotten and access to online judicial records in Laksh Vir Singh Yadav v Union of India. The Court here discussed a framework for de-indexing and masking personal information in appropriate cases. In a separate petition concerning a sexual-offence victim whose identifying details appeared in an online legal database, the Court directed instructions for immediate de-indexing and steps to prevent further disclosure and safeguards. It relied primarily on the statutory protection of the victim's identity rather than treating the case simply as a general right-to-be-forgotten claim[19].

These decisions demonstrate that Indian law contains both a general constitutional basis for privacy claims and specific legal protections for sexual-offence survivors. The two should be

[16] Justice K S Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1 (opinion of Sanjay Kishan Kaul J).
[17] Nipun Saxena v. Union of India (2019) 2 SCC 703
[18] R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.
[19] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 274–277.

applied together where appropriate, while keeping their different purposes clear. As well as balancing between RTBF with the public's right to know and judicial transparency.

The Digital Personal Data Protection Act, 2023 (DPDP Act) provides a legal framework for the processing of digital personal data in India. Section 12: This deals with the correction and erasure of personal data in certain circumstances. However, the Act came into force in different phases. Under the notification issued on 13 November 2025, Section 12 is scheduled to come into force eighteen months after the notification's publication. Therefore, as of October 2026, this provision is not yet in force[20].

Other laws provide more direct protection to sexual-offence survivors. Section 72 of the Bharatiya Nyaya Sanhita, 2023 prohibits the disclosure of the identity of victims of specified sexual offences, subject to the exceptions provided by law[21]. Earlier, the offences were governed under Section 228A of the Indian Penal Code, 1860[22].

Furthermore, the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) provides additional protection to child victims. Section 23 restricts the reporting of information that may reveal a child's identity[23]. In Nipun Saxena v Union of India, the Supreme Court also emphasised that a victim's identity can be revealed through details other than their name and hence the protection must therefore extend to information that could indirectly identify the child and their identity[24].

The Bharatiya Nagarik Suraksha Sanhita, 2023 furthermore provides for in-camera proceedings for certain sexual-offence cases, helping protect the privacy of victims and protect their identity during trial[25]. Together, these laws provide important safeguards against the disclosure of victims' identities. Although the DPDP Act addresses personal data more generally, the specific protections under criminal law and the POCSO Act are particularly relevant when a minor survivor's identity is disclosed.

[20] Digital Personal Data Protection Act 2023, s 12; Ministry of Electronics and Information Technology, Notification GSR 843(E), 13 November 2025.
[21] Bharatiya Nyaya Sanhita 2023, s 72
[22] Indian Penal Code 1860, s 228A
[23] Protection of Children from Sexual Offences Act 2012, s 23.
[24] Nipun Saxena v Union of India (2019) 2 SCC 703.
[25] Bharatiya Nagarik Suraksha Sanhita 2023, s 366.

DISTINCTION BETWEEN ERASURE, REDACTION AND DE-INDEXING

Erasure, redaction and de-indexing are different remedies for protection of a sexual abuse victim's identity.

Erasure: This refers to the deletion of personal information from a particular record or system. It may be appropriate where the information should not lawfully be retained or where the applicable legal conditions for deletion are satisfied[26]. It is not an absolute solution since it collides with the public's right to know and judicial transparency.

Redaction: This refers to hiding or removing specific details while keeping the rest of the document available. A court judgment, for example, may remain publicly accessible while the survivor's name, address and other identifying details are removed[27]. This can protect privacy without concealing the legal reasoning or outcome.

De-indexing: This refers to preventing a link from appearing in specified search results. The original webpage may remain online, but a search for the survivor's name may no longer return that link[28]. The distinction was central to Google Spain and has become important in Indian disputes involving digital judicial records[29].

These remedies should not be treated as interchangeable. De-indexing alone may be insufficient if a legal database continues to display a survivor's name directly across its database. Redaction may be more effective when the identity appears within a judgment. Erasure may be unnecessary where the document can remain accessible in a properly anonymised form. The remedy should respond to the actual source of harm and protect the survivor without removing more information than necessary. Thus, creating an appropriate balance between RTBF and judicial transparency.

[26] Digital Personal Data Protection Act 2023, s 12; Ministry of Electronics and Information Technology, Notification GSR 843(E), 13 November 2025.
[27] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 274–277.
[28] Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) EU:C:2014:317.
[29] Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) EU:C:2014:317; Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 188–191, 274–277.

LEGAL PROTECTION OF SEXUAL ABUSE VICTIMS IN INDIA

Indian law recognises that the identity of a sexual-offence survivor requires special protection. Hence, it has a structural framework to protect the sexual abuse victim's identity. Section 72 of the Bharatiya Nyaya Sanhita, 2023 prohibits the disclosure of the identity of a person against whom specified sexual offences have been committed, subject to the statutory framework. The provision continues a protection previously found in the earlier legal framework under section 228A of the Indian Penal Code[30].

The purpose of this prohibition is to prevent victims from suffering further harm. It may also discourage other survivors from reporting offences or participating in legal proceedings, fearing the harm caused due to circulation of information. The protection is therefore connected not only with individual privacy but also with access to justice.

The law also recognises limited statutory exceptions and procedures for authorised disclosure to maintain judicial transparency. Hence it must be applied according to the relevant provision rather than assumed to give publishers a general freedom to identify survivors and expose their identity[31].

The protection remains important even after a judgment has been delivered. A victim does not lose the benefit of anonymity merely because the proceedings have ended or because a judgment has become publicly available. Where an identifying document is uploaded online, the original publication may need to be corrected, masked or restricted. The legal duty must be applied to the actual disclosure, not avoided on the ground that the information has already circulated elsewhere. This is to ensure the victim can live their life freely without being haunted by their past.

Courts have repeatedly recognised that sexual-offence survivors should not be exposed to unnecessary public identification. In Nipun Saxena, the Supreme Court issued directions to ensure that the identity of a victim is not disclosed directly or indirectly. Also addressing the handling of FIRs and the use of anonymised references in legal proceedings, maintaining anonymity throughout the legal process[32].

[30] Bharatiya Nyaya Sanhita 2023, s 72; Indian Penal Code 1860, s 228A.
[31] Ibid
[32] Nipun Saxena v Union of India (2019) 2 SCC 703.

A judgment may contain the victim's personal information that makes the victim identifiable. If the judgment is uploaded to a searchable database, the same prohibited information can reach a much larger audience than intended.

The Delhi High Court's 2026 decision in Laksh Vir Singh Yadav provides a recent example. In a petition brought by a sexual-offence survivor, the Court recorded that orders and judgments containing her name and personal identifiers had been uploaded to an online legal database despite representations seeking correction. The Court directed instructions for immediate de-indexing and disabling of name-based search functionality for the material concerned. It also directed the database to introduce systems to safeguard against further issues[33]. This approach is significant because specific statutory protection should not be weakened by requiring a victim to prove that the information has become outdated or irrelevant.

Judicial anonymity protects dignity while allowing the legal system to remain open. A judgment can ordinarily continue to explain the court's reasoning, legal principles and verdict without revealing the victim's identity. The aim is not to hide the existence of sexual offences but to prevent the harm caused to the victim's life from unwanted exposure.

Children require extra protection because they may not fully understand or control what happens once their information is online. Identifiers can follow a child into adulthood and affect education, work, relationships and safety. Section 23 of the POCSO Act therefore restricts media reports that may reveal a child's identity or other relevant information which may lead to exposure of their identity, and this covers any detail that could lead to identification, not just the name[34].

Confidentiality can also be maintained through in-camera proceedings, restricted access to sensitive documents and directions on publication. A document that stays confidential during the trial can still harm if it is later uploaded without redaction, so courts and database operators should check documents before publishing them. The child's best interests should guide these

[33] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 274–277.
[34] Protection of Children from Sexual Offences Act 2012, s 23(2); Nipun Saxena v Union of India (2019) 2 SCC 703.

decisions[35]. Where a record can be made public without revealing the child's identity, anonymising it is usually more proportionate than removing the whole record.

Indirect identification means a person can be recognised from details other than their name. It could be their exact address, the school or workplace, a family relationship, a photograph, or any other small details that identify someone once they are put together[36].

This is why the harm does not really depend on whether a name appears. In Nipun Saxena, the Supreme Court said identifying details must be protected too. So, publishers and platforms have to think about what their information reveals as a whole, not just covering the mere name of the victim[37].

There is also the problem of secondary victimisation, where the survivor is hurt again by how people react to the offence. Exposure can bring blame, gossip, harassment and the same questions asked again and again, often by people who do not need to know. Online it is worse, since copies keep circulating even after the original report is corrected. What matters most is whether an ordinary reader could reasonably identify the survivor from what was published.

A survivor whose identity has been exposed has a few options to get rid of the unwanted exposure, depending on the facts and the law. The first is to write to the publisher, website or database operator and ask for the identifying details to be taken down or masked. They can also ask a search engine to de-index the link so it stops showing up for name searches[38].

If the disclosure breaks a statutory ban or a court order, the victim can go to the court and ask for directions. In some cases, constitutional remedies may also be open. The Delhi High Court's 2026 decision shows that a survivor can ask for direct relief against continued identification online[39].

A complaint should say which material is the problem, how it points to the survivor, and what law supports the request. It also helps to save the URL, screenshots and any emails, because they show the information is still there and that the earlier request got no response. Proper relief

[35] Protection of Children from Sexual Offences Act 2012, s 23; Bharatiya Nagarik Suraksha Sanhita 2023, s 366(2)–(3).
[36] Nipun Saxena v Union of India (2019) 2 SCC 703.
[37] Ibid
[38] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 188–191.
[39] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 274–277.

may mean redacting the original document, removing copies, de-indexing links, and putting safeguards in place so the material is not published again, preventing the harm.

DIGITAL EXPOSURE, DATA DISCLOSURE AND THE PERSISTENCE OF ONLINE INFORMATION

Identifying information can get out in many ways: news articles, social media posts, court documents, photographs, videos, even online discussions. Sometimes it's deliberate, while other times someone simply uploads a document and never checks whether it has protected details in it. And once it's out, people copy it and save it on other websites, causing it to circulate across multiple platforms.

This is why correcting it is so hard. A publisher can delete the original article, but the copies and screenshots are still sitting somewhere else, and search engines may go on showing the old link or description for a while. So, the survivor can still be identified even after the source has been fixed. It's worse where the law banned the publication to begin with. Nobody should have to live with continued exposure just because the information has already spread. Still, a remedy only works if it names who can actually remove or restrict the material, both in law and in practice.

Search engines make information easy to find by linking a person's name to webpages, reports and public records. That can make an identifying publication much more harmful. A report that would otherwise be hard to track down can show up the moment a survivor's name is typed into a search bar. This issue can be solved by de-indexing.

News publishers may keep old reports for historical and public-interest reasons, and legal databases give lawyers, researchers, students and the public access to judgments. These are useful things to do. But a legal database does not need to show the identity of a sexual-offence survivor where the law prohibits it and where it starts to affect the victim's lifestyle. The original record and the search result are not the same thing. De-indexing makes a page harder to find through a name search without deleting the source, and redaction removes the identifying details while the judgment's reasoning stays. In Google Spain, the Court of Justice of the European Union treated the search engine's processing as separate from the original publication. The Delhi High Court's 2026 decision also looked at the role of search engines and

legal databases in disputes over digital judicial records. So, remedies may have to go beyond the original publisher[40].

A data leak happens when information becomes accessible without proper authority or safeguards. In sexual-abuse cases, this could be an unredacted court document, an FIR uploaded by mistake, or a file which reveals the survivor's address or family details. It can also happen when someone forwards a confidential document or republishes details from another source or platform.

Republication is a further problem. Even if the original publisher takes the information down, another website may copy it, and social media users may share screenshots that the correction never reaches. Each new copy becomes another source of exposure with repeated circulation.

Responsibility should depend on the role of the person or organisation involved, the legal restrictions that apply, and what they could reasonably have done to prevent or fix the disclosure. A platform that gets a clear complaint about prohibited identifying information should have a way to look at it quickly. Where a court has given a specific direction, compliance should not have to depend upon the survivor asking again and again for their name or identity to be hidden[41].

Prevention matters just as much. Legal databases should screen documents before uploading them, use automated checks to spot personal identifiers, and have a person review sensitive cases. Automated tools cannot catch everything, especially where identity can be worked out from context, so they should support legal and editorial review, not replace it.

Public identification can affect a survivor's sense of safety, privacy and control over their personal information. It furthermore brings out unwanted messages, harassment, gossip, or pressure from relatives and the community. Survivors may also worry that a future employer, a college or an acquaintance will find out through a simple online search.

RTBF is important since these effects do not stop when the criminal case ends. A survivor who is trying to rebuild their life may be reminded of the event every time their name shows up in

[40] Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) EU:C:2014:317; Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 156, 188–189, 211–212.
[41] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 274–277, 287.

search results, and may avoid online services because they fear being identified. Not every survivor will react in the same way, and legal analysis should not assume they do. But still, the possibility of serious and lasting harm is reason enough to take identity protection seriously. In Nipun Saxena, the Supreme Court recognised the need to prevent the humiliation and social harm that disclosure causes[42].

The law should not make survivors prove that they have been subjected to extreme psychological injury before an express statutory prohibition is enforced. Where disclosure is unlawful, the duty exists whether or not the survivor can show a particular emotional response. Evidence of actual harm may still matter when choosing the remedy in a wider privacy claim[43].

Removing information from the internet is hard and difficult because different parties may control different copies. The original publisher, the website host, the search engine and the legal database may each have their own procedure, and a request to one of them does not automatically reach the others. This is especially true when the publication is circulated from one platform to another.

There is another problem. The same document can hold sensitive personal details and material of real public value. Removing the whole judgment may block access to the legal reasoning, while leaving the survivor's identity visible may break the law. Redaction and de-indexing can deal with this more precisely, but they need clear procedures and cooperation. Jurisdiction adds more trouble when a platform works across countries. A court order also has to be drafted carefully, stating the material, the action required and the time for compliance. In the end, enforcement depends on practical directions, clear responsibility, and a way for survivors to report it when the same disclosure keeps happening[44].

JUDICIAL INTERVENTION AND ENFORCEMENT OF THE RIGHT TO BE FORGOTTEN

Indian courts have recognised that protecting sexual-offence victims takes more than keeping their names out of public statements. It reaches beyond merely removing the name and also addresses the need to conceal any related information which may indirectly expose the victim's

[42] Nipun Saxena v Union of India (2019) 2 SCC 703.
[43] Bharatiya Nyaya Sanhita 2023, s 72; Indian Penal Code 1860, s 228A.
[44] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 188–189, 208–212, 286–287.

identity. In Nipun Saxena v Union of India, the Supreme Court made clear that identifying information also covers details that reveal a victim's identity indirectly. This matters a lot in digital cases, where a photograph, family details, an address or other personal information can identify a survivor even after the name is removed. Courts can order identifying details to be redacted and restrict disclosure, so that the victim's privacy and dignity are protected even after the legal proceedings have ended[45].

A judicial court order may not stop sensitive information from circulating online. News reports, copied documents, search-engine results and legal databases can continue showing identifying details even after a court has ordered them protected, and other websites may reproduce the information, making the removal of the same difficult. This is the gap between getting legal protection and having it work in practice. A survivor can win a favourable order and still be exposed, simply because the information can still be found through an online search or through indirect information online.

Publishers, digital platforms and search engines have an important part to play in stopping a victim's identity from being disclosed repeatedly. Publishers should check that their reports and court-related documents do not carry any prohibited identifying details directly or indirectly, and legal databases must make sure that what they upload follows the applicable privacy protections; furthermore, they must have a person to take action against complaints and queries raised against sensitive cases. In Laksh Vir Singh Yadav v Union of India, the Delhi High Court dealt with the online disclosure of a sexual-offence victim's identity and directed de-indexing and other steps to prevent further disclosure. The court's decision shows why practical safeguards actually matter. Even so, its directions should not be read as creating an unrestricted general right to be forgotten and must be balanced with judicial transparency[46].

Effective protection needs both immediate effective action as well as proper steps to stop the disclosure from happening again in the future. Courts can direct the platforms concerned to remove or restrict access to identifying information, and to put suitable safeguards in place so it does not reappear. Upload systems should flag prohibited details, and a person should be able to review the case where automated checks fall short. Compliance should have a set time limit, and victims should have an easy way to report these violations. At the same time, the

[45] Nipun Saxena v Union of India (2019) 2 SCC 703
[46] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 156, 274–277.

restrictions should target the identifying information, not every report about the case. That way survivors are protected while legitimate reporting and public access to information continue side by side. A court's intervention only means something when its directions lead to lasting, practical results[47].

BALANCING VICTIM PRIVACY AND DIGNITY WITH THE PUBLIC RIGHT TO KNOW

Privacy and dignity are both essential to protecting sexual-offence victims from further harm. Article 21 of the Indian Constitution protects the right to life and personal liberty, and the Supreme Court has interpreted it to include privacy[48]. In Justice KS Puttaswamy (Retd.) v Union of India, the Court recognised privacy as a fundamental right[49]. Victims of sexual abuse should have some control over how their personal information is shared, especially when disclosure of such information could expose them to stigma, harassment or unwanted attention. Protecting their identity helps keep their dignity intact and lowers the risk of secondary victimisation.

Article 19(1)(a) of the Indian Constitution guarantees freedom of speech and expression, and this includes the media's freedom to report on matters of public importance. Reporting on sexual violence can bring injustice to light, push for accountability and keep citizens informed. But freedom is not absolute. Article 19(2) of the Indian Constitution allows reasonable restrictions on certain specified grounds, as long as constitutional requirements are met[50]. A newspaper's interest in covering a case does not, by itself, justify revealing the survivor's identity or any other related information which may reveal the victim's identity. Responsible reporting can explain the facts and the legal issues without publishing details that point to the victim. Thus, even the newspaper is subject to carefully complying with victims' RTBF.

Open justice promotes transparency by letting the public see and understand how courts work and how their decisions are reached. Access to judgments and court records supports legal research, public scrutiny and confidence in the judicial system. But one must keep in mind that openness does not necessarily mean every personal detail has to be made public. Wherever

[47] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026) paras 286–288.
[48] Constitution of India 1950, art 21.
[49] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[50] Constitution of India 1950, arts 19(1)(a) and 19(2).

justifiable by law, courts can protect sensitive information through redaction, de-indexing, anonymisation or limits on access. The aim should be to keep the reasoning and outcome of a decision available while avoiding needless disclosure of a survivor's identity[51].

Public interest is not the same as public curiosity. Information about how sexual-offence cases are handled, how public authorities behave or how the law is interpreted can serve a real public purpose. Publishing a survivor's name, address, photograph or family details usually adds very little to public understanding. What it does invite is gossip, harassment and stigma. In Nipun Saxena v Union of India, the Supreme Court stressed that a victim's identity can be revealed by information other than the name[52]. Reporting should therefore stay with the relevant facts and accountability, and leave out personal details that expose survivors without enough public-interest reason.

Neither privacy nor freedom of expression should automatically win over every competing interest. A proportionate approach looks at why the information is being disclosed, whether it is really necessary, how much harm it could cause the survivor, and whether the same public purpose can be met in a less intrusive way. For example, a judgment can stay accessible while the victim's name and identifying details are taken out. The facts of each case matter, and so do any statutory limits on disclosure. This way, courts can protect privacy and dignity without needlessly restricting legitimate reporting, legal research or public scrutiny[53].

CRITICAL ANALYSIS AND COMPARATIVE PERSPECTIVES

India does not have a single, comprehensive law that deals specifically with the right to be forgotten. The protection comes from several places, which include: constitutional privacy principles, judicial decisions, data-protection law and the statutes that protect sexual-offence victims. In Justice KS Puttaswamy (Retd.) v Union of India, the Supreme Court recognised privacy as a fundamental right, but its discussion of the right to be forgotten did not create an unlimited right to erase information[54]. So, whether a removal or de-indexing request succeeds depends on the kind of information, the law that applies and the facts of the case. This can leave survivors uncertain about whether they will get consistent protection.

[51] Nipun Saxena v Union of India (2019) 2 SCC 703; R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.
[52] Nipun Saxena v Union of India (2019) 2 SCC 703.
[53] Constitution of India 1950, arts 19(1)(a), 19(2) and 21; Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[54] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

Laws such as section 72 of the Bharatiya Nyaya Sanhita, 2023 and section 23 of the POCSO Act, 2012 restrict the disclosure of the victim's identity in specified circumstances[55]. But online information can be copied, republished or made searchable by different websites or transferred from one platform to another, so victims may have to contact several platforms or go back to court for more orders. The Digital Personal Data Protection Act, 2023 gives a right to correction and erasure under section 12, but that provision is only scheduled to come into force in May 2027, and it is not in force as of October 2026. It should not, therefore, be presented as a general remedy that already works for now[56].

The European Union offers a very useful comparison. In Google Spain SL v Agencia Española de Protección de Datos, the Court of Justice of the European Union held that, in certain circumstances, individuals can ask for links to their personal information to be removed from search results that come up under their names. Article 17 of the General Data Protection Regulation (GDPR) later set out a right to erasure, with exceptions that include freedom of expression and information. This framework shows that taking down a search result does not necessarily mean deleting the original publication. For survivors, de-indexing can make identifying information harder to find, while the material that has a legitimate reason to stay available remains available. This method helps to keep the victim's information private as well as citizens' right to judicial transparency available for them to understand the legal proceedings, statutes, doctrines, and principles involved[57].

The United Kingdom applies the UK GDPR and the Data Protection Act 2018, together with protections for privacy and freedom of expression. Article 8 of the European Convention on Human Rights protects private and family life, and Article 10 protects freedom of expression. In publication cases, courts may have to balance the two very carefully. The right to erasure under the UK GDPR is not absolute, and it has exceptions for expression and information[58]. This becomes relevant to India because it shows that privacy protection has to work in practice, complying with guidelines without automatically removing every item of information about a person.

[55] Bharatiya Nyaya Sanhita 2023, s 72; Protection of Children from Sexual Offences Act 2012, s 23.
[56] Digital Personal Data Protection Act 2023, s 12; Ministry of Electronics and Information Technology, Notification No G.S.R. 843(E), 13 November 2025.
[57] Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) EU:C:2014:317; Regulation (EU) 2016/679 (General Data Protection Regulation), art 17.
[58] European Convention on Human Rights, arts 8 and 10; Data Protection Act 2018 (UK); UK General Data Protection Regulation, art 17.

India can take three lessons from these approaches. One, survivors need a clear process for asking for removal or de-indexing. Two, platforms should respond quickly to valid requests and follow what the courts direct. And three, the law should separate information that identifies a person from information the public needs to understand a case. The Delhi High Court's decision in Laksh Vir Singh Yadav v Union of India shows why practical safeguards matter against online disclosure of a sexual-offence victim's identity. Still, protecting identity under specific laws should not be confused with an unrestricted right to erase all public information[59]. This highlights the importance of maintaining a balance.

This analysis finds that the main difficulty is not that privacy protections are missing. It is that they are hard to enforce across digital platforms. Questions remain about how quickly platforms must act, how repeated uploads can be stopped, and how victims can get remedies without long proceedings. India needs clearer procedures, stronger ways of making platforms comply, and a balanced approach to removal requests. These steps would protect survivors' dignity and still keep legitimate public access to legal information.

RECOMMENDATIONS AND CONCLUSION

India needs to set up a clear procedure for survivors who want protection from the online disclosure of their identity. The procedure should separate three different remedies. Firstly: redaction, which hides identifying details in a document; removal, which deletes the material from a website. Secondly: de-indexing, which stops a link from showing up in certain search results. Each one does a different job, so the choice should depend on the circumstances of the case. Requests that involve legally protected victim identities should be dealt with first. The procedure should also make it clear where a complaint can be filed, what information has to be given and how a decision can be challenged. Clear rules would cut down the confusion for survivors and help platforms respond in a consistent and quick manner. They should make it clear as well that protecting a victim's identity does not automatically mean deleting every report or judgment about the case.

Judicial directions that protect victims should be carried out within clearly stated time limits. Every day of delay lets the identifying information spread further, and that makes later removal less effective. Courts should be able to set deadlines for redaction, removal or de-indexing,

[59] Laksh Vir Singh Yadav v Union of India W.P.(C) 1021/2016 and connected matters (Delhi High Court, 29 May 2026), paras 274–277.

depending on how urgent the disclosure is and what kind it is. Platforms and publishers should acknowledge a complaint, say what action they took, and give reasons where they cannot do what was asked. A clear reporting mechanism would also help courts check whether their directions were followed or not. If non-compliance continues, the applicable law should provide appropriate consequences for the same. These steps would help close the gap between getting a protective order and actually having privacy.

Digital platforms, publishers and legal databases should put safeguards in place so that prohibited identifying information is not published again and again. These could include checks before documents are uploaded, redaction of sensitive details, easy ways to report a problem, and quick review of complaints. Search engines should respond properly when they receive a valid legal request for de-indexing. Platforms should also take reasonable steps to stop the same material from coming back after it has been removed, without breaking the law or limiting legitimate expression. Automated tools can help with detection, but a person still has to review the case, because only the context shows whether information identifies a survivor. Accountability should depend on whether platforms actually comply. Victims should not be left to monitor the whole internet themselves.

Remedies should be affordable, easy to reach and sensitive to what survivors need. Someone seeking protection should not have to explain a traumatic experience over and over, or go to several authorities about the same disclosure. A central anonymous complaint mechanism, clear guidance and help with legal procedures would make the process easier to follow. Complaints should be handled confidentially, and extra personal information should not be collected unless it is needed. Legal aid and suitable support services may also help survivors who cannot afford long proceedings. A remedy is meant to reduce harm. It should not turn into another exhausting process for the person who came for protection before the judicial system.

Protective measures should be proportionate to the harm and the legal interests involved. Taking out a victim's identifying details can often protect privacy, and the public can still read the substance of the judgment or report. So, the restrictions should aim at the unnecessary identifying information, not at everything about a case. Courts should weigh the public interest, freedom of expression and open justice together with their statutory duties and the survivor's dignity. This balance can protect victims and still keep accountability and access to legal information.

The right to be forgotten matters especially for sexual-offence survivors, because online disclosure can prolong humiliation, stigma and unwanted exposure. Indian law already gives significant protection through constitutional privacy principles, judicial decisions and statutes that restrict the disclosure of victims' identities. But these safeguards get weaker when procedures are scattered, the same material is published again, and protective orders are hard to enforce. India needs clearer procedures for removal and de-indexing, timely compliance, responsible platform practices and remedies that survivors can actually reach without exposing their identity. Any framework must also separate genuine public interest from the unnecessary disclosure of personal details. A survivor's identity should stay protected without them having to fight repeated exposure online themselves. A fair and practical system has to uphold privacy and dignity and still keep legitimate public access to information.