

Right to Be Forgotten in India: Balancing Privacy and the Right to Information

Ishita

LL.M., GD Goenka University

ABSTRACT

The rapid spread of the internet has altered the way personal information is produced, stored, searched and shared. Details that once stayed within a small local or social circle can now be reached anywhere in the world in a matter of seconds. This supports free expression, research and public accountability, but it can also inflict lasting harm when information that is outdated, irrelevant, misleading or deeply sensitive stays easy to find long after the event it describes. The right to be forgotten has developed as a legal answer to that problem. In general terms, it is a person's ability, in suitable circumstances, to ask for the removal, restriction or de-indexing of personal information whose continued public availability is no longer necessary or proportionate. In India the right is closely tied to the constitutional right to privacy as recognized in Justice K.S. Puttaswamy (Retd.) v. Union of India. It is, however, not absolute, and has to be weighed against freedom of speech and expression, the public's right to know, press freedom, open justice and the preservation of public records. This paper looks at the constitutional basis of the right to be forgotten, the relevant judicial decisions, the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025. The right to be forgotten covers the erasure of personal data, the de-indexing of search results and the suppression of original public records. The paper contends that India requires a clear, transparent and proportionate framework built on the nature of the information, the lapse of time, the position of the person concerned, the public interest and the risk of harm. Such a framework should safeguard personal dignity without letting privacy claims turn into a means of censorship or of rewriting history.

Keywords: Right to be Forgotten, Right to Privacy, Right to Information, Article 21, Article 19(1)(a), Digital Personal Data Protection Act, 2023, Data Erasure, De-indexing, Informational Privacy, Public Interest.

1. INTRODUCTION

The internet has produced a lasting digital record of what people do. News reports, court judgments, social media posts, photographs, employment records and other personal details can stay searchable for years. A person may have been acquitted, may have served a sentence, or may have moved well past an earlier episode, yet a search of their name can still bring up the old material. The outcome can amount to a permanent digital punishment that affects work, education, relationships and participation in society. The right to be forgotten addresses this concern by asking whether personal information should stay accessible in the same form, and to the same degree, without any time limit.

The idea does not mean that anyone can insist on the complete deletion of every fact about their life. It is better seen as a qualified claim to control how long certain personal information remains available.

Depending on the facts, the fitting remedy might be deletion, correction, anonymization, restriction of processing or de-indexing from a search engine. These remedies are not the same. De-indexing can make a result harder to find through a name search while the original webpage or public record stays untouched. Erasure, on the other hand, involves deleting data held by a particular controller, subject to exceptions provided by law.

The question is especially significant in India because constitutional privacy and freedom of expression are both strongly protected. Article 21 protects life and personal liberty, which include dignity and privacy. Article 19(1)(a) guarantees freedom of speech and expression, and Article 19(2) allows only specified reasonable restrictions on it. Article 19(1)(a) also bears on the public's access to information, although the right to information is not unlimited and can be subject to legitimate privacy interests. Public access to judicial decisions, journalism and historical records can be vital for accountability. Yet the online circulation of intimate or obsolete information may be out of proportion to any purpose the public still has in it.

The central difficulty, therefore, is how to strike a balance between privacy and information in each case. The aim is to build a principled method for doing so. This paper examines the Indian constitutional framework, judicial developments and the statutory position, and suggests safeguards for a fair system of deciding requests to be forgotten.

2. STATEMENT OF THE RESEARCH PROBLEM

The main problem is that no single, fully settled and comprehensive judicial test exists to decide when a person may require that personal information be removed or made harder to reach online. Indian courts have dealt with requests from acquitted persons and requests concerning sensitive personal details and court records, but the results depend heavily on the facts and the type of material. The Digital Personal Data Protection Act, 2023, creates rights over personal data, including correction, completion, updating and, in specified circumstances, erasure, but it does not create an unlimited constitutional right to wipe all information from the internet.

Matters become harder when a request touches a public record or information that still matters to public debate. Someone may seek privacy because a report embarrasses them, while journalists, researchers or ordinary citizens may argue that the same information is needed for accountability. Too much removal can hide wrongdoing, weaken open justice and erode the public record. A policy of refusing every request, though, can leave individuals exposed to disproportionate and indefinite harm. The legal task is to find fair criteria, effective remedies and procedural safeguards that protect privacy without handing private parties control over public history.

3. OBJECTIVES OF THE STUDY

The first objective is to examine the legal basis and present standing of the right to be forgotten in India. The study seeks to explain how privacy under Article 21 relates to expression and access to information under Article 19. It reviews the important judicial decisions that have shaped the Indian approach, among them Justice K.S. Puttaswamy (Retd.) v. Union of India, Dharamraj Bhanushankar Dave v. State of Gujarat, Jorawar Singh Mundy v. Union of India, and Subhranshu Rout v. State of Odisha. It also considers the relevance of the Digital Personal Data Protection Act, 2023, and the rules notified in 2025. Another objective is to tell apart erasure, anonymization, suppression of records and search engine de-

indexing. Lastly, the paper puts forward criteria and institutional safeguards for resolving competing claims in a transparent and proportionate way.

4. RESEARCH QUESTIONS

1. What does the right to be forgotten mean, and how far does it extend, in the Indian legal system?
2. In what way does the right to be forgotten flow from the constitutional right to privacy under Article 21?
3. How should privacy be weighed against freedom of expression, the right to information and open justice?
4. Which principles can be drawn from Indian judicial decisions on online personal information and court records?
5. What part do the Digital Personal Data Protection Act, 2023, and the 2025 Rules play in protecting personal data and permitting erasure?
6. What legal and procedural safeguards can prevent arbitrary censorship and still give effective relief to people suffering disproportionate digital harm?

5. RESEARCH HYPOTHESIS

The right to be forgotten can be accepted as a qualified element of informational privacy in India, but its exercise should be governed by a transparent proportionality test. That test would look at the sensitivity and accuracy of the information, the time that has passed, the person's public role, the continuing public interest and the likely harm from continued accessibility. A balanced, case-specific framework fits constitutional values better than either automatic deletion or a blanket refusal to remove information.

6. RESEARCH METHODOLOGY

The paper follows a doctrinal and analytical method. It draws on primary legal materials, namely the Constitution of India, judicial decisions, the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025. Secondary sources, such as legal commentary and academic writing, are used to explain the wider debate. The study is qualitative and involves no field surveys or statistical analysis. It examines the principles stated by courts and in legislation, points out areas of uncertainty and develops recommendations grounded in constitutional privacy, proportionality, freedom of expression and public accountability. The legal position is stated as of October 2026; when considering when particular provisions of the DPDP framework take effect, the applicable commencement notifications and the phased implementation schedule must be consulted.

7. MEANING AND SCOPE OF THE RIGHT TO BE FORGOTTEN

In broad terms, the right to be forgotten is a person's ability, in appropriate circumstances, to seek limits on the continued publication, processing or easy retrieval of personal information. It rests on the thought that a person's identity should not be fixed forever by one past event, and that information gathered for one purpose need not remain open for every conceivable purpose indefinitely.

The expression takes in several separate legal remedies. The first is erasure, meaning that an organization deletes the personal data it holds where the law permits or requires this. The second is de-indexing, which removes a link from the results produced by a search engine, usually for searches on a person's name; the source webpage may still be reachable directly. The third is anonymization, which

alters information so that the person can no longer be identified, for instance by taking a name out of a sensitive judgment. The fourth is restriction of processing, which limits how data may be used without deleting it altogether. The fifth is correction, which may suit cases where the information is inaccurate or incomplete.

These remedies should not be treated as interchangeable. Asking for a database entry to be deleted is very different from demanding that a court judgment be erased from the public record. Similarly, taking down a search result can lessen harm without stopping journalists or researchers from reaching a legitimate source. The remedy ought to fit the problem. Where information is false, correction or a right of reply may work better than deletion. Where intimate details are needlessly exposed, redaction or anonymization can protect privacy while keeping the legal reasoning intact. Where a lawful public record still matters for accountability, even de-indexing calls for scrutiny and should not be granted automatically.

The right also differs from a right to rewrite history. It cannot ordinarily be invoked merely because someone dislikes truthful information or wants to hide matters of continuing public importance. Its strongest basis appears where information is inaccurate, highly intrusive, no longer relevant to its original purpose, or available in a way that causes serious and disproportionate harm.

8. CONSTITUTIONAL FRAMEWORK IN INDIA

Article 21 provides that nobody may be deprived of life or personal liberty except by procedure established by law. The Supreme Court has read this provision widely so as to protect dignity, autonomy and aspects of privacy. Informational privacy is about a person's ability to exercise some control over how information about them is collected, used and circulated. The right to be forgotten can be argued to arise as one facet of this protection, especially where continued online availability weakens dignity or autonomy without adequate justification.

Article 19(1)(a), by contrast, protects freedom of speech and expression. It safeguards the ability to publish, receive and discuss information. Journalism, academic research, historical records and access to judicial decisions all feed public debate and accountability. Any restriction on expression must fall within the constitutional scheme, including the grounds listed in Article 19(2). A court or authority that considers a removal request must therefore take care not to impose a broad restriction only because the information is uncomfortable or damaging to reputation.

The right to information rests on democratic principles, and the Supreme Court has recognized it as linked to freedom of speech and expression. It lets citizens judge the conduct of government and take a meaningful part in public affairs. Even so, access to information does not automatically defeat every privacy claim. Intimate medical details, information about survivors of sexual violence, or facts about private individuals may carry little real public value even though they are technically available online.

The constitutional task is to balance the rights through legality, legitimate purpose, necessity and proportionality. The Puttaswamy judgment explains that privacy is not absolute and that any intrusion must meet suitable constitutional safeguards. Applied to the right to be forgotten, this means that neither the individual's request nor the public's claim to information should be accepted without examining the context. The identity of the person, the source of the information, its accuracy, the nature of the proceeding, the time that has passed and the public importance of the record all count.

9. LANDMARK JUDICIAL DECISIONS

9.1 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

In this landmark decision of a nine-judge bench, the Supreme Court unanimously held privacy to be a fundamental right under the Constitution. The Court linked privacy to dignity, liberty and personal autonomy and explained that it has informational dimensions. The judgment did not create an unlimited or fully worked-out right to be forgotten, but it supplies the constitutional foundation on which claims about control over personal information can be built. It also makes plain that privacy is not absolute and that restrictions must satisfy constitutional requirements.

9.2 Dharamraj Bhanushankar Dave v. State of Gujarat (Gujarat High Court, 2015)

The petitioner asked the court to stop the online publication of a High Court judgment in a criminal appeal. The Gujarat High Court did not accept the arguments put forward, having regard to the relevant court rules and the public character of judicial decisions. The case matters because it shows that a litigant's wish to prevent online access does not by itself justify suppressing a judgment. Open justice and the integrity of public court records are weighty considerations on the other side. The decision reminds us that the right to be forgotten has to be reconciled with the legal rules on access to judgments.

9.3 Jorawar Singh Mundy v. Union of India (Delhi High Court, 2021)

The petitioner had been acquitted in a criminal case, yet the judgment kept appearing in online searches and allegedly harmed his career prospects. The Delhi High Court granted interim protection, directing that the judgment be removed from certain search results or be blocked from access through search engines until the matter was considered further. The case drew attention to the harm that can follow when an acquittal is overshadowed by the continued online visibility of earlier allegations or proceedings. The order was interim and tied to its facts; it should not be taken to lay down an automatic rule that every judgment concerning an acquitted person must be deleted. Its importance lies in recognizing that privacy and practical harm need to be considered alongside public access.

9.4 Subhranshu Rout v. State of Odisha (Orissa High Court, 2020)

This case arose from objectionable images and videos of a woman and the alleged non-consensual circulation of intimate material. The Orissa High Court discussed the right to be forgotten in connection with privacy, dignity and protection from continuing online harm. It shows why removal mechanisms can be particularly important where intimate content is circulated without consent. Such cases are unlike requests to remove accurate reporting in the public interest, since the material may directly violate personal dignity and may have little legitimate public value. The decision supports the need for prompt and sensitive remedies, especially for victims of online abuse.

9.5 Other High Court approaches

High courts have heard applications seeking removal or masking of names in judgments dealing with matrimonial disputes, sexual offenses, acquittals and sensitive personal facts. The results are not wholly uniform. Some decisions have allowed redaction or limited online discoverability in particular circumstances, while others have stressed open justice and the public nature of judgments. These decisions suggest that the Indian position has grown step by step through case-by-case adjudication and not through a single comprehensive judicial test. The continuing variation strengthens the argument for clear statutory and procedural guidance.

10. RIGHT TO INFORMATION, OPEN JUSTICE, AND FREEDOM OF EXPRESSION

The right to information is basic to democratic accountability. Citizens need access to public records in

order to see how courts, governments and public institutions use power. Judgments set out legal principles, allow scrutiny of judicial reasoning and help keep the law consistent. Journalists and researchers likewise depend on archived material to look into patterns of conduct and to document public events. If all embarrassing or adverse information could be taken down whenever the person concerned asked, public records might become incomplete and accountability might suffer.

At the same time, open justice does not require every personal detail in every record to be permanently searchable by anyone. A judgment may include addresses, medical details, information about children, sexual history or other sensitive facts that are not needed to follow the legal reasoning. The public interest may lie in the legal outcome and reasoning, not in the continued exposure of someone's identity. Redaction, anonymization and limits on name-based indexing can sometimes preserve transparency while cutting down needless harm.

A helpful distinction is that between the public interest in the underlying information and the public interest in a particular way of reaching it. A record may rightly stay in a court archive, but a search engine's instant link between a person's name and an old case creates a different scale of exposure. The remedy should therefore ask whether the information has to be erased or whether a narrower step can protect privacy adequately.

The person's role also matters. Information about public officials carrying out public duties, candidates for public office or conduct involving public funds may carry a stronger continuing public interest. A private individual's unrelated intimate information, on the other hand, may deserve greater protection. Even public figures keep their privacy rights; public status does not turn every part of private life into a legitimate matter of public concern.

The balance must not be flattened into a simple choice between reputation and transparency. Truthful reporting can cause damage and still serve a public purpose. Conversely, information that is technically accurate can become misleading if it leaves out a later acquittal, correction or change in circumstances. In such cases, adding an update, linking to the outcome or correcting the record may be more proportionate than taking down the original publication.

11. DIGITAL PERSONAL DATA PROTECTION ACT, 2023, AND RULES, 2025

The Digital Personal Data Protection Act, 2023, sets up a statutory framework for processing digital personal data in India. It recognizes the rights of individuals, called Data Principals in the Act, and the obligations of entities that decide the purpose and means of processing, known as Data Fiduciaries. The Act tries to balance an individual's interest in protecting personal data against the need to process such data for lawful purposes.

Section 12 is of particular relevance as it deals with rights relating to correction and erasure of personal data. It gives individuals a statutory route to seek correction, completion or updating of personal data, and erasure in the circumstances the Act lays down, subject to applicable legal requirements and retention obligations. The right is not an unconditional power to remove every reference to oneself from every website. How it operates depends on the statutory text, the purpose for which the data is processed, the duties that apply and the exceptions the law recognizes.

The Digital Personal Data Protection Rules, 2025, were notified in November 2022. The Act and Rules have a phased commencement framework, so it should not be assumed that every provision became operational on the date of notification. The relevant commencement notifications must be checked when

a particular provision is applied. This matters academically because the enactment of a statute and the coming into force of an individual provision are separate legal questions.

The DPDP framework can strengthen personal data governance by setting expectations on lawful processing, transparency, security and the rights of individuals. The statutory right to erasure and the wider constitutional debate on a right to be forgotten are, however, not the same thing. The former works inside a data-protection regime and relates to personal data processing covered by the Act. The latter can involve search engine indexing, publication by news organizations, court records and constitutional claims that do not fit neatly into a single data-controller relationship.

Public records and legal obligations raise a further point. Data may have to be kept in order to comply with the law, perform public functions or preserve records. A request for erasure must therefore be assessed alongside the applicable retention duties and legitimate public purposes. The framework should not be read as allowing the deletion of evidence or the destruction of official records contrary to law.

The most accurate conclusion is that the DPDP Act forms an important part of India's emerging data-protection architecture and offers relevant rights and obligations, but it does not answer every question linked to online reputation, court judgments or public-interest reporting. Judicial balancing and clear procedures remain important.

12. INTERNATIONAL PERSPECTIVE

The international debate is commonly associated with the European Union's data-protection framework and the decision of the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014). There the Court considered whether search engines could be required, in certain circumstances, to remove links to information shown in the results of a search on a person's name. The case separated the search engine's role in organizing and making information accessible from the original publisher's role in publishing it. It helped establish the idea that de-indexing may be appropriate even where the original webpage is not deleted.

European data-protection law recognizes a right to erasure in specified circumstances, but it also contains exceptions and calls for balancing against freedom of expression, public interest and legal obligations. The European approach should not be copied mechanically in India, which has a different constitutional text, institutional structure, data-protection framework and history of public access to judicial records. Even so, the distinction between deleting source material and limiting name-based search results is a useful one.

International experience indicates that the right works best when it is framed as a contextual remedy and not as an automatic entitlement. It also underlines the value of transparent criteria, review procedures and careful handling of public figures, journalism, historical research and information about criminal proceedings. India can learn from these models while developing a framework consistent with its own constitutional values.

13. KEY CHALLENGES IN INDIA

To begin with, the standards applied by different courts and platforms are uncertain. Different courts, kinds of information and procedural settings can lead to similar requests being treated differently. Secondly, the internet is hard to regulate on a territorial basis. Even if one platform removes a result,

copies may remain on other websites, archives or servers outside India. Thirdly, powerful individuals may misuse requests in order to suppress accurate reporting on matters of public importance.

A fourth challenge is practical: working out who should receive a request. The original publisher, website host, search engine, court registry and data fiduciary may perform different functions and may not bear the same legal responsibility. Fifth, removal can clash with record-preservation requirements, evidentiary needs and the public's interest in historical accuracy. Sixth, victims may face delay, cost and procedural complexity when trying to stop the spread of intimate content or of information that puts them in danger.

It is a further difficulty that the passage of time does not automatically make information irrelevant. An old report about a public official may stay important, whereas an older private detail may have lost almost all public significance. Accuracy matters too: a record that reports an allegation but leaves out a later acquittal can give a misleading impression. The law must therefore look at context, updates and the actual harm caused instead of relying on age alone.

14. PROPOSED FRAMEWORK FOR BALANCING THE RIGHTS

A fair Indian framework should start with a structured proportionality assessment. The factors below should be weighed together and not applied as rigid, isolated rules.

First, accuracy and completeness: is the information false, misleading, outdated or incomplete? If a correction or update can solve the problem, deletion may be unnecessary. Second, sensitivity: does the material disclose intimate, medical, sexual, financial or child-related information? Highly sensitive material generally calls for closer scrutiny. Third, public interest: does the information concern public office, public funds, serious misconduct, public safety, a legal precedent or an issue of continuing social importance? Fourth, the person's role: is the person a private individual, a public official, or someone who voluntarily entered public debate? This factor is relevant but never decisive on its own.

Fifth, passage of time and later developments: has the person been acquitted, has an allegation been disproved, has a sentence been served, or has the information otherwise lost relevance? Sixth, the likely harm: is the information causing serious and continuing consequences such as harassment, threats, discrimination or loss of livelihood? Seventh, the source and legal status of the record: is it a court judgment, a news article, a social media post, a public register, or personal data held by an organization? Eighth, the availability of less restrictive measures: could redaction, anonymization, a correction, a contextual note or de-indexing give enough protection without deleting the source?

Procedural safeguards are just as important. Platforms should offer an accessible request process, acknowledge requests promptly and give reasons for their decisions. Requests concerning intimate images, minors or immediate safety risks should have an expedited route. Requests involving public records or public-interest journalism should be reviewed with care and should not be granted solely because a person objects to adverse publicity. Where a request is contested, an independent review mechanism or a judicial remedy should be available.

The process should protect both sides. The person seeking relief should be able to explain the harm without having to republish sensitive information unnecessarily. Publishers and affected third parties should get a chance to respond where appropriate. Reasons for decisions should be recorded, and the decisions should be consistent with constitutional standards. A transparent process can reduce arbitrary removal and build public trust.

Finally, the remedy should be narrow. If the harm comes from a person's name appearing in search results, de-indexing may be more proportionate than deleting a court judgment. If a judgment carries unnecessary sensitive details, redaction may be suitable while the legal reasoning is preserved. If a post contains false personal data, correction may be the best response. A flexible remedy is more likely to protect privacy while keeping public information intact.

15. FINDINGS OF THE STUDY

The study arrives at the following findings. First, the right to be forgotten in India is closely bound up with informational privacy and the constitutional values of dignity and autonomy, particularly after the Puttaswamy judgment. Second, it is not an absolute right and cannot serve as a general device to suppress truthful information or rewrite public history. Third, the decisions of Indian High Courts show the importance of context: cases about acquittals or intimate material raise different concerns from requests to remove ordinary public judgments or reporting in the public interest.

Fourth, the right to erasure under the DPDP Act, 2023, is significant but does not settle every question about search engines, public records and freedom of expression. The Act and Rules must be read with their commencement provisions and applicable exceptions. Fifth, de-indexing, anonymization, correction and deletion are distinct remedies and should not be treated as interchangeable. Sixth, legal certainty would improve with a transparent proportionality test, accessible procedures, reasoned decisions and independent review. Finally, the most balanced approach protects personal dignity without damaging open justice, journalism and democratic accountability.

16. SUGGESTIONS AND RECOMMENDATIONS

India should develop clear statutory or judicial guidelines that identify the factors relevant to right-to-be-forgotten requests. The guidelines should expressly separate erasure of personal data from de-indexing of search results and from the removal or alteration of official public records. They should offer stronger and quicker protection for intimate images, minors and information that creates a serious safety risk.

Search engines and online platforms should put accessible complaint systems in place and give reasoned outcomes. A review mechanism should exist for cases where a request is rejected or where removal could affect information of public interest. Courts should consider narrow remedies, such as anonymization or de-indexing, before ordering the deletion of an entire judgment or publication. Public authorities should preserve official records in accordance with law while limiting needless disclosure of sensitive personal details.

Training and awareness are needed as well. Individuals should understand the difference between an inaccurate report, a privacy violation and truthful reporting in the public interest. Platforms should explain what kinds of evidence are required and how far any remedy extends. Researchers, journalists and courts should use redaction practices where personal identifiers are not required to understand the issue. These steps would help India build a system that is practical, fair and constitutionally sound.

17. CONCLUSION

The right to be forgotten has become an important issue in the digital age because the internet can preserve and circulate personal information long after its original relevance has faded. Persistent searchability can expose people to disproportionate harm and can interfere with privacy, dignity and the

chance to move on in life. Yet unrestricted removal of information can threaten freedom of expression, the public's right to know, open justice and the preservation of historical records.

The Indian constitutional framework gives a basis for balancing these interests. The Puttaswamy judgment recognizes privacy as a fundamental right, while freedom of expression and democratic access to information remain essential constitutional values. High Court decisions show that requests have to be judged in context. The Digital Personal Data Protection Act, 2023, and the Rules notified in 2025 are important developments in the regulation of personal data, but the right to erase personal data should not be mistaken for an unrestricted right to erase public information from the internet.

The most suitable course is a qualified and proportionate right backed by transparent standards and effective procedures. Decision-makers should weigh accuracy, sensitivity, public interest, the person's role, the passage of time, later developments, the harm caused and the availability of less restrictive remedies. De-indexing or anonymization may often protect privacy while leaving the underlying public record accessible. Strong safeguards are needed to prevent both needless exposure and censorship.

In the end, the purpose of the right to be forgotten should not be to erase history. It should be to make sure that personal information is not kept or made accessible in a manner that is unjustified, excessive or disproportionate. A carefully balanced framework can protect individual dignity while preserving the openness and accountability that a democratic society needs.

18. REFERENCES

A. Constitutional and Statutory Materials

1. Constitution of India, Articles 19(1)(a), 19(2), and 21.
2. Digital Personal Data Protection Act, 2023, especially Section 12.
3. Digital Personal Data Protection Rules, 2025, notified in November 2025, read with the applicable commencement notifications.
4. Information Technology Act, 2000, and applicable rules, where relevant.

B. Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. Dharamraj Bhanushankar Dave v. State of Gujarat, Gujarat High Court, 2015.
3. Jorawar Singh Mundy v. Union of India, Delhi High Court, 2021.
4. Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878.
5. Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, Court of Justice of the European Union (2014).

C. Official and Secondary Sources

1. Ministry of Electronics and Information Technology, Government of India, "Digital Personal Data Protection Rules, 2025," official publication, 14 November 2025.
2. Press Information Bureau, Government of India, "Government notifies DPDP Rules to empower citizens and protect privacy," 14 November 2025.
3. Delhi High Court, orders in Jorawar Singh Mundy v. Union of India.
4. Gujarat High Court, decision in Dharamraj Bhanushankar Dave v. State of Gujarat.
5. Orissa High Court, Subhranshu Rout v. State of Odisha.

Note: Case citations and statutory commencement details should be checked against official court and Gazette copies before formal submission. The paper uses the law and publicly available material located for the purpose of this academic draft. This ensures that all referenced legal precedents and regulations

are accurately represented and aligned with the current legal framework. Furthermore, diligent verification of sources will enhance the credibility and reliability of the research presented.