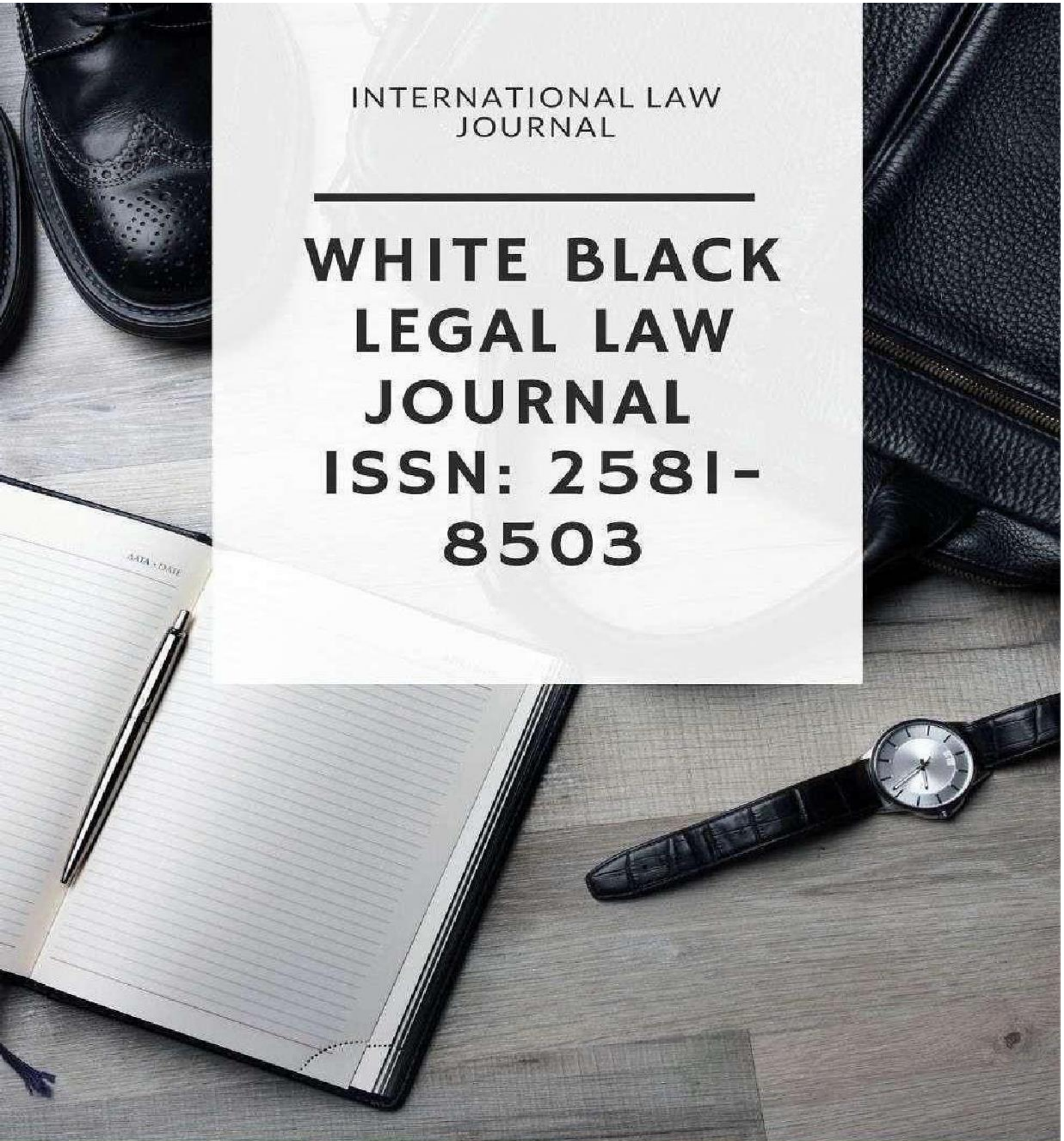




INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

AN ANALYTICAL STUDY ON PRIVACY OF PERSONAL DATA WITH SPECIAL REFERENCE TO ARTIFICIAL INTELLIGENCE AND CYBER SECURITY IN INDIA

AUTHORED BY - LOKESH

Abstract

The right to privacy, rooted in Article 21 of the Indian Constitution, has become an essential facet of personal liberty in the digital era. With the advent of artificial intelligence (AI) and the rapid growth of cyber technologies, safeguarding personal data has emerged as both a constitutional necessity and a global challenge. This study undertakes an analytical exploration of privacy and data protection in India, contextualized within AI and cybersecurity frameworks. It traces the historical evolution of privacy from ancient Indian traditions and colonial jurisprudence to its constitutional recognition by the Supreme Court in landmark cases such as *Kharak Singh*, *Gobind*, and *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The research highlights the dual nature of AI—its capacity to enhance efficiency while simultaneously raising concerns of mass surveillance, algorithmic bias, automated profiling, and data breaches. It critically examines contemporary regulatory responses, including the EU's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023, evaluating their strengths, limitations, and implications for businesses and individuals. Case studies such as *Aaradhya Bachchan v. Bollywood Times* and corporate data misuse incidents underscore the urgent need for robust frameworks. The paper concludes that privacy must be integrated as a fundamental value in digital governance, requiring transparent practices, ethical AI development, and strong enforcement mechanisms. By balancing innovation with accountability, India can foster trust, protect fundamental rights, and ensure security in the evolving cyber era.

Keywords: Privacy, Artificial Intelligence, Cybersecurity, Data Protection, India

Introduction

Originating from the Latin "privatus," the English term "privacy" denotes "separated from others, deprived of something, office, or participation in governance." Ensuring everyone lives in peace, dignity, and freedom is the purpose of Article 21 of our Indian Constitution, and privacy is the best method to achieve this. Ensuring data security and protection is both a national concern and a fundamental right as our nation continues its gradual digitalization. These are essential components of privacy when using the internet.

and we are entering what many have called a "Cyber Era." Also, there is a very crucial and delicate region in the law right now where data protection and privacy are interdependent.

The increasing prevalence of online activities creates new security risks to personally identifiable information, heightening the importance of protecting users' privacy and secrecy. Thanks to "big data" technologies, massive data volumes may now be processed quickly.², quickens the massive gathering of data. The owners of the individual databases may be able to extract sensitive information if they combine them. The widespread gathering of data from many devices and sources, such as computers and smartphones, exacerbates this problem.

Data misuse by individuals having access to data for organizational objectives and, consequently, the necessary authorizations to access sensitive or private information, is a major concern in this context due to the inherent danger. Data privacy and secrecy, however, are subsets of data security.³ Important decision-making relies on accurate data, therefore keeping it secure is crucial. Ensuring the security of data is of utmost importance. In order to achieve data security and privacy, strategies for secure authentication methods

are crucial.⁴ The terms "privacy" and "rights" have been defined differently by different researchers.

The definition of privacy given by **Black's Law Dictionary** is the "*right to be left alone; right of a person to be free from unwarranted publicity; and right to exist without unwarranted intervention by the public in things with which the public is not necessarily concerned.*"

Inherent in every human being is the right to privacy, which has many benefits but also gives rise to certain exceptions. We fight against crossing the boundary between privacy and secrecy. Based on this, it's safe to assume that everyone has set limits on how they want to be approached in their personal lives.

Most people today agree that Article 21's right to life and personal liberty includes the right to privacy as an essential component. Article 21's right to life, according to a wide reading, includes more than only the ability to live and the necessity of doing so. One of the many things

that gives a man a feeling of meaning in life is the right to privacy. A person has the right to privacy if they want to be alone. Everyone has the right to keep their private information about themselves, their families, their marriages, their children, their schooling, and their reproduction and motherhood under wraps.

According to **D.D. Basu**, “*The term privacy is too broad, and it encompasses not only seclusion from neighbors. Imagine it as a circle that no government should be able to cross; it encompasses every individual.*”⁵

The definitions demonstrate that there is a lack of consensus among scholars and lawyers regarding the nature of privacy. On the other hand, here is a brief explanation of the right to privacy::

1. Everyone has an innate need for some personal space where they may relax knowing no one will pry into their affairs.
2. Concepts of privacy vary between nationalities, cultures, customs, and historical periods.
3. Western intellectuals see the right to privacy as an umbrella term for a variety of protections, in contrast to Indian intellectuals who take a more holistic approach. On the other hand, according to Indian scholars, privacy is essentially a singular noun meaning exclusion.

Origin and Historical Evolution of Concept of Privacy

Although people have always had the right to privacy, it wasn't until the 20th century that this right was widely recognized. This is proven by the countless works of political and religious literature that have been written all around the globe. As an example, the Arthashastra, an Indian architectural text, lays forth regulations for house design according to the need for privacy. A person's house has to be built far enough away from nearby houses, according to these criteria. Additionally, he needs to secure the doors and windows.

The restriction of utilizing someone else's property without their approval in the Yajnavalkya, Samhita, and Manusmriti is only one more example of how highly ancient people regarded the right to privacy in one's own space and assets. Further, mental independence was bestowed when the Arthashastra suggested specific woodland locations as venues for contemplation leading to enlightenment. In ancient Mesopotamia, the Hammurabi Code made it illegal to enter someone's house without their permission. It was also against the law in Rome to go into someone else's home. Still, throughout those primitive eras, privacy had a very definite

meaning. Evidence from studies of social structure and animal behavior suggests that the need for solitude may have evolved from an earlier, more primal state.⁶

In Modern Era Development of Concept of Privacy

Contemporary societies' views on personal privacy vary according on the prevailing political system in any given country. The political structure greatly affects the way the state implements its privacy and surveillance programs. There is a spectrum that modern nations can be positioned along, ranging from democracies to totalitarian governments. How political systems determine what is private can be understood by comparing cultural norms on this spectrum.

Governments that lean toward totalitarianism often keep a close eye on their citizens. Governments in both China and Russia are notoriously tight-lipped when it comes to their inner workings. The individualism thesis is rejected by these states, which consistently prioritize requirements of the nation prioritizing individual welfare. The practice of eavesdropping, collecting personal information about individuals, and espionage has thus been normalized in these nations⁷

In opposition to states leaning toward totalitarianism, democratic states rely on individualistic ideology. In most cases, personal liberties trump governmental protections. Due to the democratic preeminence of individual rights, the right to privacy has evolved into a fundamental human right in contemporary societies. Privacy, both personal and collective, is therefore essential in modern democracies, in contrast to totalitarian regimes where such practices are inevitable for the sake of state purposes.

A liberal democratic state is based on the premise that individuals' lives can be improved via the use of freedom and chance..⁸The two concepts are interchangeable in these states: privacy and freedom. In all aspects of their lives—mental, emotional, spiritual, social, and moral—they aim to grant their citizens the right to privacy. The inherent constraints of privacy on free speech in contemporary democracies make it all the more urgent to strike a fair balance between the two rights..⁹ This means that in modern democracies, when the state's interests take precedence over individual ones, the right to privacy can nonetheless be subject to legitimate limitations.

Legal Development of Right to Privacy: Indian Position

This right to privacy is guaranteed to Indian citizens by both property laws and the Indian Penal

Code. These regulations, similar to the British legal system, protected individuals' rights to person and property by trespass and defamation prohibitions, respectively. All of these instances revolve around the idea of personal property rights, particularly as they pertain to a person's house. A mountain of evidence suggests that the right to privacy was already well-established in India prior to its 1890 American citation.

This idea initially appears in decisions made by courts prior to their independence. The judges of the Sardar Diwani Adalats and the British India Courts made these rulings. It was in the 1855 decision of North-Western Province in Nuth Mullin that the concept of privacy initially arose.¹⁰ In light of the decision of Delhi's principal Sadar Amin, Begbie, Smith, and Jackson filed an appeal.

Based on the defendant's construction of a new house that, from its rooftop, overlooked the plaintiff's property, infringing on the plaintiff's right to privacy, JJ found that the plaintiff had a case against the defendants in this instance.. Chief Justice Edge addressed this issue in Gokal Prasad(1888)¹¹, where the court made the observation that due to the destruction of documents after the 1857 insurrection, it was impossible to determine if this region of India had a tradition of privacy.

It is difficult to tell whether the judges of the Sadar Diwani Adalat of the North-Western Provinces relied on the law as it was discovered to be in effect at the time or relied on the evidence available because the subject was never established or contested before 1855 and there is a lack of information on the subject in the report of the Nuth Mull and KureemOolah Beg case.

C.J. Edge mentioned a variety of privacy cases in the Gokal Prasad case. In Gunga Prasad (1862)¹², Ross and Roberts, JJ, did not raise any doubts about the existence of a right to privacy. In the Goor Das v. Banaras (1867)¹³ and Ram Baksh v. Moradabad case (1867)¹⁴, Morgan C.J. and Spankie J. explicitly acknowledged the validity of a right to privacy.

Whether a home in Allahabad might have a right to privacy was reviewed by JJ. Straight and Mahmood in a case from 1886. Prof. Winfield¹⁵ In order to persuade the House of Commons to allow British residents the right to privacy, it was necessary to cite Indian precedents from 1931. Clauses pertaining to trespassing and defamation give this right. As a result, property rights were given undivided attention. At the time, the country was under British dominion, therefore fully recognizing the right to privacy would have been against its interests. The right to privacy was not safeguarded by Indian law since the government of India adopted British principles upon independence..

Constituent Assembly Response: Right to privacy

The "Right to Privacy" was deemed an essential right during the drafting of the Indian Constitution. This is according to what Fundamental Right Committee member Mr.

R. K. Sidhwa has said., "Although the Constituent Committee argued for the protection of private correspondence and the prohibition of interception of letters, telegrams, and telephones, this provision was later repealed by the Main Committee.¹⁶ Distinguished members of the Fundamental Rights Sub-Committee, such as K.M. Munshi, had proposed: "Here are some rights that every person should have: a) the right to know, within 24 hours, who is taking away his freedom and why; b) the right to live in peace and quiet in his own home; c) the right to have his correspondence kept private; and d) the right to be protected from exploitation that goes against public morality or the law by means of Union law."¹⁷

"No one has the right to invade someone's privacy by searching their home, person, or property without a warrant," said Dr. B.R. Ambedkar. "Warrants cannot be issued without first establishing probable cause, which must be proven by oath or affirmation. The warrant must also detail the location to be searched as well as the individuals or property to be confiscated."¹⁸ On the other hand, fierce animosity ensued in response to these privileges. Since every private letter would become a state paper or record concerning State activity under the confidentiality of correspondence, Alladi Krishnaswami Ayyar was opposed to it.

B. N. Rau held the view that "if there is no search without a court's order, it may adversely undermine the powers of investigation of the police." This view led him to oppose the constitutional right to privacy. Upon becoming aware of the theft, a police officer surveys the area, giving them a chance to reclaim the loot.¹⁹ But the time it takes to petition for a court warrant and provide all the necessary paperwork could be fatal due to the distance and lack of transportation in rural India. Granting such a right, he argued, would make it difficult to administer justice in a country the size of India. In the end, nevertheless, the Constitution did not include it.

Constitutional Response: Right to Privacy

Notably, the Indian Constitution does not guarantee a right to privacy in and of itself. The right to personal privacy is not included in a list of fundamental rights. However, courts have often considered the different aspects of the right to privacy and upheld it under the right to life, which is a fundamental right protected by Article 21 of the Constitution, and under various other provisions of the Constitution when read with the Directive Principles of State Policy. In

Kharak Singh (1963)²⁰, In the case of the disputed UP Police Regulations, the first Prosser tort—the invasion of privacy—was maintained by the US Supreme Court. The petitioner was first held on suspicion of dacoity but was subsequently released due to a lack of evidence. The police found his history sheet and put him under monitoring. Police Regulation UP 236 states: "Domiciliary visits at night, covert picketing of suspects' homes or approaches to their homes, etc." The petitioner challenged Regulation 236 included in Chapter XX of the UP Police Regulation. A number of courts affirmed the rule's constitutionality. A minority decision by Justices Subba Rao and Shah found that home visitation monitoring, together with other types of surveillance, infringed the subject's right to privacy under Article 21. Therefore, the possibility that the Right to Privacy could be deduced from other basic rights was finally acknowledged.

The Supreme Court conducted a more thorough analysis of the right to privacy in *Gobind* (1975)²¹. The validity of a rule that mandated monitoring over many channels specified in that rule was examined. The court upheld the rule. A "process established by law" determination means that the rule does not violate Art. 21. Art. 19(1)(a), (d) and 21's temporary right to privacy has been recognized by the Court. It was also decided that the reasonable limitations mentioned in Art. 19(5) of the Constitution do not impact this privilege.

In the landmark *Gobind* case, the Indian Supreme Court upheld an individual's right to privacy. *Pooranmal* (1974)²¹, Due to the absence of an unambiguous fundamental right to privacy, the Court determined that evidence gathered through unlawful searches cannot be rejected on the grounds that they infringe upon personal private. There were less safeguards against warrantless searches and evidence seizures as a result of this decision. Also, people's right to privacy was downplayed.. In the case of *V.S. Kuttan Pillai* (1980)²², A search would not be considered an invasion of privacy, according to the Supreme Court's ruling, even if no results were returned because of competing government interests..

The Supreme Court stated in *R. Rajgopal* (1994)²³ it is implicit in the right to life and liberty that all persons are guaranteed by Article 21, and the right to privacy has only achieved constitutional status. Individuals' right to privacy is acknowledged. "The right to protect one's own, family, marriage, procreation, motherhood, childbearing, and education, among other topics," according to the document. Although the right to privacy and the freedom of speech and expression are sometimes at conflict, the court was able to find a middle ground. Aside from the explicit guarantees of life and liberty in Article 21, the Court reasoned that Americans also had an implied right to privacy.

Another example of an invasion of privacy is the tapping of telephones, which dealt with the

disclosure of information. The Supreme Court ruled in *R. M. Malkani* (1973)²⁴ that the courts would shield a law-abiding citizen's phone conversation from an overbearing government agency's prying ears. Protection was granted, even though it was unrelated to the right to privacy.

In *People's Union for Civil Liberties (PUCL)* (1997), the Supreme Court revisited the question of whether or not it is permissible to intercept telephone calls.²⁵ The court reached the conclusion that the right to privacy is an element of the rights to "life" and "personal liberty," which are protected by Article 21 of the constitution, as was established in the present instance. The right to privacy is protected under Article 21 when the facts of a particular case warrant it, and it cannot be curtailed "unless by the procedure prescribed by law." The ability to assert or establish a violation of the right to privacy depends on the particular facts of the case. As the Court has already said, "telephone talk is an integral aspect of man's private life." Undoubtedly, one can invoke a "right to privacy" to defend the capacity to speak on the phone in total secrecy at home or at the office. This means that Article 21 prohibits the illegal practice of tapping a person's phone without a warrant or other official authorization. "Just, fair, and reasonable" is the requisite nature of the procedure."

According to Section 5(2) of the Telegraph Act of 1885, In India, it is lawful to tap a person's phone. The Court has ruled that this portion is legitimate under the Constitution. This section lays forth the circumstances and reasons for when a warrant can be issued to conduct a telephone tapping. The Court has ruled that the Indian Constitution, specifically Article 19(2), permits the tapping of telephones for the purposes specified therein.²⁶ The right to privacy in cases involving the disclosure of personally identifiable information has been upheld by courts in recent years. Claims of unlawful disclosure that infringe upon the right to privacy are often heard by the Court and decisions are made on them.

As the court pointed out in the *Indu Jain* case, a claim for right to privacy can only be brought against governmental instrumentalities.²⁷ (High Court of Delhi, 12th October 2007), on the basis of a violation of the plaintiff's right to privacy, filed a lawsuit seeking an injunction order to prevent the defendants from publishing the plaintiff's name in *Forbes'* list of Indian billionaires. Nevertheless, the order did imply in subsequent paragraphs that the guidelines would provide protection for privacy, even though no statute specifically grants such a right. Nevertheless, the court in this case ruled that the right to privacy of famous persons is limited due to the fact that the public finds it interesting to learn about them and journalists have the freedom to publicize their names.

When it came to revealing information necessary to protect another person's fundamental rights

or the public good, however, the court had no qualms about ruling against the right to privacy.. The Supreme Court held in *Mr. X (1999)*²⁸ according to the Directive Principles of State Policy and other sections of the Constitution pertaining to Fundamental Rights, the "right to privacy" has been removed.. The appellant's claims were denied by the court, however it did note that those rules violate the right to privacy. Having said that, the right is not inviolable and could be curtailed by law. In situations where two basic rights are at odds with one another, such as this one involving one party's right to privacy as part of their right to life and another party's right to live a healthy life, both of which are fundamental rights under Article 21, the court process would only enforce the right that would advance public morality or the public interest. This is because it is impossible to censor moral considerations."²⁹.

In *Sharda (2003)*³⁰, A medical examination ordered as part of a divorce proceeding is not considered an invasion of privacy as it is essential for proving a claim. The highest court in the land has decided that there are some situations where the ban on invasion of personal privacy in Article 21 of the Constitution does not apply. The right that advances public morality would be prioritized if it were to conflict with another party's fundamental right. Because of this, public policy imperatives were able to supersede private interests in this case. As if the Indian court had acknowledged, even in a limited way, the right to privacy today. By Government Resolution dated 22/02/2000³¹, In order to examine the Constitution's inner workings, the government established a National Commission. Without changing the document's essential framework or features, the objective was to propose any essential changes to the Constitution's clauses.³²In reference to the right to privacy, the Commission had proposed adding an additional article labeled 21-B to the line that follows, "Art. 21-B," as the right to privacy is stated in Article 21, according to the Supreme Court's ruling. The right to privacy includes the freedom to write, live in one's own house, and spend time with one's family. (2) The State may, for reasons such as public safety, the prevention of disorder or crime, the protection of health or morals, or the protection of other people's rights and freedoms, pass laws that reasonably limit the exercise of the right granted by clause (1) notwithstanding anything in clause (1).

Concerns about AI and data protection laws

From the way we use technology to the way businesses function, artificial intelligence (AI) has revolutionized many parts of our lives. The increasing sophistication and widespread use of AI, however, brings up serious worries over data protection and privacy regulations.

1. **Increased data collection and processing:** Companies are collecting and processing more data because AI systems need it for training and making decisions. This presents a number of privacy concerns, such as:
 - **Unlawful or unethical data collection:** Companies can violate people's right to privacy if they gather data without their knowledge or consent.
 - **Data profiling and behavioural targeting:** AI has the potential to build comprehensive profiles of individuals through their internet activities; these profiles might then be utilized for targeted advertising or surveillance purposes..
 - **Algorithmic discrimination:** Discriminatory results in domains like healthcare, credit scoring, and employment could be caused by AI algorithms that reinforce and reinforce existing biases.
2. **Automated decision-making and profiling:** Loan approvals, employment applications, and insurance coverage are just a few examples of the kinds of decisions that AI-driven systems may make autonomously. This makes one wonder if decision-making procedures are open and accountable.:
 - **Lack of explainability:** The decision-making process and the considerations taken into account by AI algorithms might be difficult to decipher because to their complexity and opaqueness.
 - **Bias and discrimination:** Unfair or discriminating results could be the result of automated decision-making systems unintentionally incorporating biases or mistakes.
 - **Right to explanation:** A person's right to ask for an explanation of how AI-driven judgments impact their life is not necessarily put into practice.
3. **Governmental use of AI for surveillance and law enforcement:** There are serious privacy concerns associated with the widespread use of artificial intelligence (AI) by governments for purposes of surveillance and law enforcement.:
 - **Mass surveillance:** Many are worried about the potential invasion of privacy and restriction of movement brought about by surveillance systems driven by artificial intelligence (AI) that can gather and analyze massive volumes of data from public areas.
 - **Facial recognition technology:** There are legitimate worries over the possibility of abuse, fraudulent identity, and lack of consent with regard to facial recognition technology, notwithstanding its usage in identification and

law enforcement.

- **Predictive policing:** Predicting and identifying possible offenders through the use of AI algorithms brings up ethical questions around profiling and the possibility of prejudice.
4. **Data security and privacy breaches:** Data breaches and unauthorized access to sensitive information can occur when AI systems are themselves the targets of cyberattacks. Cyberattacks can also be made more targeted and sophisticated with the use of AI technologies.
 5. **Legal frameworks and regulations:** Existing legal frameworks and regulations aimed at protecting data and privacy have not kept up with the lightning-fast advancements in AI. As a result, rules and regulations vary widely from one jurisdiction to another, posing difficulties and unknowns for businesses and individuals alike³³.

Things google did for privacy regulation

The usage of public data sets in training models

AI primarily learns from massive volumes of publicly available personal information. Name, phone number, and shipping address are all pieces of this info. Laws that have been in place for a while adapt to new situations as AI operates like a complex network. The phrase is typically linked to data collection, processing, and access in the context of legal privacy. The main point is to figure out when data is public and may be utilized by anyone, and when it's personal and should be secured. Protecting sensitive information and upholding individuals' privacy rights depend on this differentiation³⁴.

Privacy regulation with new AI

Governments around the world are currently concentrating on ways to comply with current privacy regulations and enact new ones. There must be careful consideration of the potential overlaps and interactions between these new regulations and the most recent AI policy initiatives. Included in the most recent executive order on artificial intelligence (AI) development and use are regulations pertaining to privacy, security, innovation, equity, and the interplay between privacy legislation and AI.

Children's privacy regulation

Children's Online Privacy Protection Act (COPPA) concerns data collected from U.S. children under the age of thirteen and its subsequent usage. Regulatory frameworks for this sector are to be determined by the Federal Trade Commission. Their goal is to make sure that while making AI, developers and manufacturers give serious thought to the collection of data from kids and how their system will interact with them.

Make privacy a core element of the basic structure of the company

All regulatory compliance and investments in technology should adhere to privacy standards, which allow for efficient and frequent privacy practices.

Simplify compliance

Employees should be held accountable by the firm for ensuring privacy compliance.³⁵

GDPR (General Data Protection Regulation)

Regarding privacy and security, the General Data Protection Regulation (GDPR) has been the most typically embraced statute. Any entity that gathers and handles personal information of EU or non-EU residents is required to comply with this regulation, which the EU enacted. Giving people more say over their own data is one goal of the General Data Protection Regulation (GDPR). It has no bearing on the physical location of the website. Companies must disclose to consumers the purposes for which they are using their personal information.

Highlights of GDPR

- General purpose of GDPR-The gathering and standards for evaluating persons' personal data are laid out in the legislation. Customers have the right to know how businesses are making use of their personal information. It doesn't matter where the business is located; it's applicable everywhere.. The law states that companies cannot mislead consumers with vague and confusing language; thus, they must ensure.
- Notification- Website visitors should be informed about the data gathering.
- Lawfulness and transparency- The business must be transparent about how it uses customer data and follow the regulations set out by GDPR to ensure compliance.
- Purpose limitation- The express and lawful goal of collecting personal data is of the utmost importance. No data will be utilized for incompatible purposes; however, the

business may store the data for future use in statistical analysis, public interest research, or scientific study.

- Data minimisation- In order to collect and process personal data, the organization must ensure that it is relevant, adequate, and limited to what is necessary for the objectives at hand. Unnecessary personal data should never be collected by the organization.
- Accuracy of data-The data must be updated on a regular or periodic basis by the organization. Organizations are required by law to promptly delete any personally identifiable information that is either erroneous or cannot be changed. Immediate and appropriate action must be made to rectify the data.
- Storage limitation- When a person's personal information is no longer needed, the controller in charge of it must erase it. Since no time restriction is specified, the controller is free to store the data indefinitely or create an archive if the data's intended use is for public or scientific purposes. Employees are informed about the retention term and the specific method utilized for computation by the organization³⁶..

Digital Personal Data Protection Act 2023

In light of the landmark Supreme Court decision in the case of, the act aims to design new laws *Justice K.S. Puttaswamy (Retd) vs. Union of India* which cast doubt on the veracity of the Aadhar Scheme in protecting citizens adequately in light of current privacy regulations.

The act was assented to by the president after being enacted by both chambers of parliament on August 11, 2023. Nevertheless, the formal gazette publication will announce when this act becomes effective.

Essential points of DPDP Act, 2023

- It covers all types of personal information that are perceived digitally, whether they are digital or not.
- Both Indian data subjects and the goods and services provided by Indian data controllers are affected by the overseas processing of data.
- In accordance with the DPDP Act, the data will be processed lawfully.
- It is important to gather only relevant data.
- There are no subsets of personal data; the DPDP is applicable to all of them.
- The organizations will make the choice to consent available. In addition to being

unrestricted and clear, it should be explicit and detailed.

- Any time personal information is requested, the data principal must be notified. The person has the right to revoke consent if they are helped properly with the request. The data principal is obligated to comply with additional languages as specified in the Eighth Schedule of the Indian Constitution in addition to notice and consent.
- Data fiduciaries must compel compliance with the DPDP Act. For example, – Unless the government notifies a restriction on data transfers, data fiduciaries are free to send data across borders as they see fit.
- As an enforcement organization, the Data Protection Board of India has the authority to issue receipts for personal data breaches, investigate breaches, apply penalties, check documents, call individuals, and require them to appear before it, according to its constitution. Any decision made by the DPB can be appealed to the Telecom Disputes Settlement and Appellate Tribunal ('TDSAT'). The TSAR might face an appeal in India's highest court.
- For reasons of public interest, the federal government can request data from a data fiduciary or intermediary and then order the public to be unable to access any computer source containing that data. Following the opportunity to be heard, the order will be issued in writing³⁷.

Exemption under the DPDP ACT

- within the bounds of Indian sovereignty, that is, in service of the general welfare and the preservation of law and order, litigation, case law, claims, mergers, amalgamations, investigations, prosecutions, etc.
- private, household, or professional journalistic objective.
- Offence and penalties- Under this act, the authority may levy heavy penalties on data fiduciaries for various offences
 1. not following the rules and not carrying out its responsibilities
 2. breach of the data processing requirements of this law
 3. Penalties for non-notification to the board might exceed Rs 5 crore, which is equal to 2% of the global turnover of the fiduciary penalty.

Positive side of data protection laws in business and corporations.

- Data transfer overseas- Any personal information kept within the country can have a copy kept by a data fiduciary. This stops vital data from being sent outside and helps

safeguard national interests from foreign threats. But the board gets to decide how to handle sensitive information and personal details.

- Trust tool- Fintech and BFSI organizations are stepping up their technical and administrative processes to guarantee compliance. Companies in the BFSI and fintech industries must adhere to their current applications, and their policies can easily adjust to new privacy regulations. Companies should think about the extra expenses that may arise from complying with rules, even though a solid privacy policy might increase customer trust.
- Forensics- Computer forensics is the most important system that is impacted by electronic discovery. The processing of computer forensics investigations, however, requires prior agreement, as stated in the legislation. The business would have to hire the right lawyers to conduct forensic analyses in the event that an innocent employee or employees are falsely accused of noncompliance.
- More demand for privacy skills- Experts and specialists in data protection will be in high demand in the digital sector, where the position is expected to play a pivotal role.
- Data portability- Without hesitation, the law grants the right to data portability to another data fiduciary.
- Special glimpse for sensitive data- A data fiduciary must have explicit written authorization from an individual before processing any personally identifiable information (including sensitive data) by means such as letter, email, or fax. Only for certain welfare and social protection programs may personally identifiable information be disclosed.
- Notification of breach-The data controller has a 7-day window after discovering a breach to inform the affected individual and anybody with the power to mitigate the damage.
- Improving business- Customers will place greater trust in company operations once the act is notified and implemented.
- Reduction- It will increase the act's transparency while decreasing crime and corruption.
- Improving security-Businesses can feel more secure and corporations can improve their market standing by respecting employees' right to privacy.
- Brand protection- Businesses can lay the groundwork for integrating IT security policies strategically while they brace for disaster. A strategic opportunity for brand success exists in safeguarding client privacy.³⁸

Negative side of data protection laws for businesses and corporations

- Compliance- Regulations, documentation, and administrative duties that are required for compliance can add time and money to the process.
- Effects on startups and companies- To identify instances of fraud, businesses employ data analytics. Conflicts of interest can be discovered, for instance, by comparing information on small businesses and vendors to those of workers.
- Effect on digital forensics- Organizations are compelled to get consent for such forensic analysis when investigating employees for noncompliance.
- Technical and process change- Online platforms are obligated to assist customers with their right to be forgotten and right to correction requests by providing an assessment of their personal data.
- Additional cost of employment -To make sure they're following all the rules and regulations, businesses should hire data security officers.
- Limitation- Processing data for these purposes requires explicit, relevant, and valid consent.
- Time-consuming- In order to save time, the organization that requested KYC Aadhar verification using the internet portal will have to redesign the process to be physical. To comply, businesses must use the standard procedure, which requires less personal information.
- Impact on communication services- The huge tech corporations are held accountable for any breach of privacy practices by WhatsApp and Facebook, which are private companies performing public functions.
- Job portals- Information technology rules of 2000 do not apply to the data collected from employment portals, which includes personal information, contact details, and professional credentials. A modification for such behaviors can now be enforced thanks to this statute.
- Matrimonial websites- Data protection regulation aims to combat threats on matrimonial sites that might lead to serious privacy violations, such as the sale of data to third parties, theft, or illegal leakage of data..
- Insurance sector- Data security and privacy in the insurance industry are paramount because of the volume of sensitive information stored there. Nevertheless, the fundamental issue of privacy rights is disregarded..
- Banking and M-wallets-Banking and M-wallets are in a similar predicament as the

insurance industry. We must not lose sight of the idea of consumer privacy laws. Regulations for the maintenance of client privacy can be improved through data protection laws.

Cases on data protection

Justice K.S. Puttaswamy and Anr vs. Union of India (2018)

Though constitutional, the Aadhaar Act—passed as a "Money Bill"—and its use of mandatory identification for state assistance schemes were considered by the Supreme Court in this case. The required Aadhaar and PAN card links are defined under Section 139 AA of the Act, and the court has maintained this ruling as lawful.

Rochem Separation System Pvt. Ltd. v. Nirtech Pvt. Ltd. and Ors. (2022)

The Bombay High Court issued an ex parte order prohibiting the former employee from using proprietary information while employed there. Before leaving for his new job, the former employee saved client information, pricing information, and other sensitive files on his own device. Using the data he had downloaded, he subsequently called the former client of the company. The former worker went so far as to recruit coworkers to his new firm.

Aaradhya Bachchan & Anr vs. Bollywood Times and Ors. (2023)

Aradhya Bachchan is suing the government, claiming that she was falsely portrayed as a crippled youngster. In a landmark decision, the Delhi High Court has warned the public to refrain from using Non-Consensual Intimate Images (NCII) and other personally identifiable information.

The court made it clear that intermediaries must comply with the removal of NCII content upon obtaining the court order and guarantee the online protection of individuals³⁹.

AI-related privacy concerns: real-life example

The age of artificial intelligence (AI) has brought with it a rise in privacy issues. The overreach of large tech businesses, who own extensive personal data, is a prime illustration of this.

A recent incident in my own life brought these worries to light. Using my Apple TV, I watched an Amazon Prime program. I got news recommendations about the show two days later when using an iPhone Google app to search. I find this incidence especially troubling because I never used my iPhone to watch the show or conduct any searches connected to it.

This situation raises several privacy issues.

Firstly, The interdependence of different systems and tools is seen here. Amazon Prime recorded my viewing habits and connected them to my Google account, even though I used a variety of devices and services—possibly without my awareness or permission.

Secondly, It implies that large digital businesses might be participating in secret data sharing or tracking methods. I may have unwittingly had my data shared across platforms as I got show-related news recommendations on another device and platform.

Thirdly, This occurrence brings attention to the possibility of personalized content and targeted advertisements that are derived from our online actions. While tailored suggestions might be helpful and improve usability, they also bring up issues of privacy invasion and monitoring.

A comprehensive strategy is needed to resolve these privacy issues. The tech industry as a whole has to be more transparent and accountable for the way it handles consumer data. Protecting users' personal information can be achieved by the implementation and enforcement of strong privacy legislation. It is important to inform users about the potential privacy risks associated with the technologies and services they use. Making people more aware of data tracking and sharing methods can help them make better judgments about what they do online. People can have more say over their data if we build tools and technologies that protect their privacy. One way to lessen the impact of data collecting and sharing concerns is to provide encryption, anonymization, and opt-out alternatives.

In sum, regulators, tech companies, and consumers must work together to address the privacy issues caused by Big Tech's intrusive activities in the AI era. We may strive for a more equitable and privacy-conscious online environment by being open and honest, honoring users' permission, and providing them with information and resources⁴⁰.

Conclusion

Last but not least, data protection and privacy standards are changing fast, especially in the AI industry. More and more people are worried about how AI will gather, handle, and exploit their personal data as the technology develops. There is an urgent need for strong privacy protections due to the explosion of AI-powered apps, such as virtual assistants and facial recognition systems.

Legislation such as India's Digital Personal Data Protection Act (DPDP Act) and the EU's General Data Protection Regulation (GDPR) are major strides in giving people agency over their own data. As a result of these regulations, businesses must be forthright about the

information they gather, get customers' permission before doing anything, and keep their data safe and accurate.

Despite the fact that these rules are necessary safeguards for customers, they pose difficulties for organizations and businesses. Investments in technology, people, and process modifications are often necessary for compliance initiatives. While more established organizations have to deal with complicated regulatory environments, startups and smaller businesses may have it worse.

But there are possibilities among the difficulties. Businesses can increase their brand reputation and customer loyalty by embracing privacy standards, which enhance trust between customers and businesses. Furthermore, by boosting cybersecurity measures and fostering ethical data-driven processes, strict data protection laws encourage innovation.

But lawmakers, companies, and people all need to be on the lookout for new privacy issues and ways to adapt to technology developments. We can fully utilize AI's promise while protecting essential rights and values in the digital era if we find a middle ground between innovation and privacy protection.

REFERENCES

Books

- D.D. Basu, *Commentary on the Constitution of India* 4772 (59th edn., LexisNexis, India, 2015).
- Alan F. Westin, *Privacy and Freedom* 8 (Atheneum Publication, New York, 1970).
- Margaret Mead & Elena Calas, "Child-Training Ideas in a Post-Revolutionary Context: Soviet Russia," in Margaret Mead & Martha Wolfenstein (eds.), *Childhood in Contemporary Cultures* 179, 190–91 (University of Chicago Press, Chicago, 1955).
- Hannah Arendt, *The Human Condition* (Doubleday Anchor Books, New York, 1959).
- Morroe Berger, Theodore Abel et al., *Freedom and Control in Modern Society* 190 (D. Van Nostrand Company, New York, 1954), available at https://archive.org/stream/in.ernet.dli.2015.498862/2015.498862.Freedom-and_djvu.txt (last visited on Aug. 17, 2025).

Journal Articles

- Yashraj Bais, "Privacy and Data Protection in India: An Analysis," 4(5) *International Journal of Law Management & Humanities* 1793–1804 (2021),

<https://doi.org/10.1000/IJLMH.112146>.

- P. Gyanchandani Jain, M. Khare & N. Big, “Data Privacy: A Technical Perspective and Review,” 3 *Journal of Big Data* 25 (2016), <https://doi.org/10.1186/s40537-016-0059-Y>.
- Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey & Christopher Millard, “The Rise of Cyber Security and Its Impact on Data Protection,” 7(2) *International Data Privacy Law* 73–75 (2017), <https://doi.org/10.1093/idpl/ipx009>.
- Indu, Rubesh Anand & Vidhyacharan Bhaskar, “Identity and Access Management in Cloud Environment: Mechanisms and Challenges,” 21 *Journal of Electrical Systems and Information Technology* 574–588 (2018), <https://doi.org/10.1016/j.jestch.2018.05.010>.

Primary & Government Sources

- “AI and Privacy: The Privacy Concerns Surrounding AI, Its Potential Impact on Personal Data,” *The Economic Times* (Apr. 25, 2023), available at <https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms> (last visited on [August 10,2025]).
- “Privacy,” *The Economic Times*, Topic Overview, available at <https://economictimes.indiatimes.com/topic/privacy> (last visited on [[August 10,2025]).
- “3 Things Privacy Professionals Should Consider at the Intersection of AI and Data Privacy” (Google Checks Team), *Google AI Blog* (Feb. 5, 2024), available at <https://blog.google/technology/ai/google-checks-data-privacy-ai-update/> (last visited on [[August 10,2025]).
- “What is GDPR, the EU’s New Data Protection Law?” *GDPR.eu* (guide website), available at <https://gdpr.eu/what-is-gdpr/> (last visited on [[August 10,2025]).
- “General Data Protection Regulation (GDPR),” *Investopedia*, available at <https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp> (last visited on [[August 10,2025]).
- “Recent Cases on Data Protection and Privacy in India,” *BananaIP Counsels Intellegedia* (Aug. 22, 2023), available at

<https://www.bananaip.com/intellepedia/data-protection-privacy-recent-cases-india-law/> (last visited on [[August 10,2025]]).

- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), (Ministry of Electronics and Information Technology, Government of India), available at <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf> (last visited on [[August 10,2025]]).
- **“Supreme Court Judgment on Privacy and Its Effect on Business,”** *ICSI Journal*, available at https://www.icsi.edu/media/filer_public/a7/39/a739c660-11ac-429d-b151-ae3e3b22b6a4/supreme_court_judgement_on_privacy_and_its_effect_on_business.pdf ((August 10,2025)).
- Constituent Assembly of India Debates (Proceedings), Vol. III (Apr. 29, 1947), available at <https://164.100.47.194/Loksabha/Debates/Cadebatefiles/C29041947.html> (last visited on Aug. 17, 2025).
- Government of India, “Report of the National Commission to Review the Working of the Constitution (NCRWC),” *Ministry of Law and Justice*, available at [https:// www.legalaffairs.gov.in/ncrwc-report](https://www.legalaffairs.gov.in/ncrwc-report) (last visited on Aug. 17, 2025).

¹ Yashraj Bais, *Privacy and Data Protection in India: An Analysis*, 4 (5) IJLMH Page 1793 - 1804 (2021), DOI: <https://doi.org/10.10000/IJLMH.112146>

² Jain.P.Gyanchandani, M& Khare, N.Big Data Privacy: A Technical perspectiveand Review. J Bi g Data3,25(2016), hppt://doi.org/10.1186/s40537-016-0059-y

³ Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, Christopher Millard, The rise of cyber security and its impact on data protection, *International Data Privacy Law*, Volume 7, Issue 2, May 2017, Pages 73–75, <https://doi.org/10.1093/idpl/ipx009>

⁴ I, Indu& Anand, Rubesh& Bhaskar, Vidhyacharan. (2018). Identity and access management in cloud environment: Mechanisms and challenges. 21. 574-588. 10.1016/j.jestch.2018.05.010.

⁵ Basu D.D, “*Commentary on the Constitution of India*”4772 (LexisNexis, India, 59thedn., 2015

⁶ Alan F. Westin, *Privacy and Freedom* 8 (Atheneum Publication, New York, 1970).

⁷ Margaret Mead and Elena Calas, “Child-training Ideas in a post-revolutionary context: Soviet Russia”, in Margaret Mead and Martha Wolfenstein (eds.), *Childhood in contemporary Cultures*, 179, 190-191 (University of Chicago Press, Chicago, 1955)

⁸ Hannah Arendt, *The Human Condition* (Doubleday Anchor Books, New York, 1959

⁹ Morroe Berger and Theodore Abel, *et.al., Freedom and Control in Modern Society* 190 (D. Van NostrandCompany,NewYork,1954),availableat:<https://archive.org/stream/freedom-and-djvu.txt> (last visited on August 17, 2025)

¹⁰ Nuth Mull v/s Zuka-Oolah Beg Sr.D.A.N.W.P.R.1855, P.92

¹¹ Gokal Prasad v.Radho ILR Allahabad (10), 358 (1888), p. 384.

¹² Gunga Prasad v. Salik Prasad S.D.A.N.W.P. Rep. 1862 Vol. II, 217

- ¹³ Goor Das v. Manohar Das N.W.P.H.C. Rep. 1867, 269
- ¹⁴ Ram Baksh v. Ram Sookh N.W.P.H.C. Rep. 1867, 269
- ¹⁵ Percy H. Winfield, "Privacy" 47, L.Q.R. 29-30 (1931)
- ¹⁶ 'Constituent Assembly of India Debates (Proceedings)-Vol. III', 29 April 1947, available at <https://164.100.47.194/Loksabha/Debates/Cadebatefiles/C29041947.html> (Last visited on August 17, 2025)
- ¹⁷ Rao, B. Shiva, (ed.), *The Framing of India's Constitution*, (ULP, Agra, 2015)
- ¹⁸ Rao, B. Shiva, (ed.), *The Framing of India's Constitution*, (ULP, Agra, 2015)
- ¹⁹ Rao, B. Shiva, (ed.), *The Framing of India's Constitution*, (ULP, Agra, 2015)
- ²⁰ Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295
- ²¹ Gobind v/s State of Madhya Pradesh AIR 1975 SC 1378
- ²² V.S. Kuttan Pillai v. Ramkrishnan AIR 1980 SC 185
- ²³ R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632
- ²⁴ R.M.Malkani v/s State of Maharashtra AIR 1973SC 157
- ²⁵ People's Union for Civil Liberties v/s Union of India AIR 1997 SC 568
- ²⁶ PUCL v. Union of India (1997) 1 SCC 301
- ²⁷ Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006)
- ²⁸ Mr. X v. Hospital Z AIR 1999 SC 495, (1998) 8 SCC 296
- ²⁹ Mr. X v. Hospital Z AIR 1999 SC 495, (1998) 8 SCC 296
- ³⁰ Sharada v. Dharampal, (2003) 4 SCC 493
- ³¹ www.legalaffairs.gov.in/ncerwc-report (Last visited on August 17, 2025)
- ³² www.legalaffairs.gov.in/ncerwc-report (Last visited on August 17, 2025)
- ³³ AI and Privacy: The Privacy Concerns Surrounding AI, Its Potential Impact on Personal Data," *The Economic Times*, Apr. 25, 2023, available at <https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr> (last visited on August 5, 2025)]
- ³⁴ "Privacy," *The Economic Times*, Topic Overview available at <https://economictimes.indiatimes.com/topic/privacy> (last visited on [May 5, 2025]).
- ³⁵ 3 things privacy professionals should consider at the intersection of AI and data privacy" (Google Checks Team), *Google AI Blog*, Feb. 5, 2024.
- ³⁶ General Data Protection Regulation (GDPR)," *Investopedia*, available at <https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp> (last visited on May 5, 2025)
- ³⁷ Recent Cases on Data Protection and Privacy in India," *BananaIP Counsels Intellepedia*, available at <https://www.bananaip.com/intellepedia/data-protection-privacy-recent-cases-india-law/> (last visited on August 5, 2025)]
- ³⁸ The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), (Ministry of Electronics and Information Technology, Government of India), available at <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> (last visited on August 5, 2025)
- ³⁹ Recent Cases on Data Protection and Privacy in India," *BananaIP Counsels Intellepedia*, available at <https://www.bananaip.com/intellepedia/data-protection-privacy-recent-cases-india-law/> (last visited on August 5, 2025)]
- ⁴⁰ Supreme Court Judgement on Privacy and Its Effect on Business," *ICSI Journal*, available at https://www.icsi.edu/media/filer_public/a7/39/a739c660-11ac-429d-b151-ae3e3b22b6a4/supreme_court_judgement_on_privacy_and_its_effect_on_business.pdf (last visited on [August 10, 2025])