JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 20

Data Piracy and Enforcement Mechanisms in India

Gunjan Arora

Faculty of Law, Jai Narain Vyas University

Recommended Citation:

Arora (2026) "Data Piracy and Enforcement Mechanisms in India" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 20. (DOI)

ABSTRACT

Data Piracy is a serious, evolving threat to the Indian Economy. In today's digital world, piracy takes place in both online and offline forms. The discussion about data piracy and its enforcement in India shows the clash between personal rights and digital evolution. This research aims to explore the current legal framework in India on data piracy. It will analyse, explain, and compare the existing laws, including the Digital Data Protection Act, 2023, and the European Union's General Data Protection Regulation.

The paper will first examine the current legal protections against data piracy in India, including the Information Technology Act, 2000, its amendments, the SPDI Rules, 2011, and the Digital Data Protection Act, 2023. Then, it will look at the Constitutional basis for data protection through landmark judgments such as Shreya Singhal v. Union of India (2015) and Justice K.S. Puttaswamy v. Union of India (2017). After that, it will critically evaluate and compare the Digital Personal Data Protection Act, 2023, with international standards like the GDPR. Finally, the study will offer recommendations to improve the current laws on data piracy in India by addressing existing gaps.

KEYWORDS

Data piracy, Digital Personal Data Protection Act, Information Technology Act, Copyright Act, General Data Protection Regulation.

INTRODUCTION

In its simplest form, Data refers to facts and statistics that are not processed. Personal data is the information that is used to identify individuals. When this information is stored and shared electronically, it is called digital data. In today's world, the protection of this data is important for ensuring individuals' rights.

What is generally referred to as data piracy is the act of unauthorized copying, distribution, or use of digital content. In today's interconnected world, this illegal activity represents one of the most pervasive and damaging challenges faced by industries across the digital economy.[1]

Data piracy was never an issue, but as technology grows, data privacy has become a matter of concern. The digital revolution has changed the way of data storage, processing, and sharing. As more people engage online, the risk of data piracy also increases.

Data piracy refers to unauthorised copying, use, or distribution of digital content. Data piracy leads to serious consequences, such as, it results in identity theft, financial losses, and harm to people's reputations. India is particularly vulnerable to data piracy. The rapid growth of high-speed internet and file-sharing technologies has made it challenging to enforce laws against piracy. Pirates often operate anonymously, using encrypted networks and peer-to-peer systems to conceal their identities. The internet connects people around the world, making it more difficult for law enforcement to intervene.

India's digital economy is expanding quickly, but the country faces major challenges in protecting sensitive digital information. Meanwhile, regions like the European Union have strong laws, such as the General Data Protection Regulation (GDPR), to combat data piracy. India is working to improve its data protection laws. This paper will examine India's current legal framework related to data piracy. The traditional data protection framework in India, including the Information Technology Act of 2000, and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 (SPDI Rules, 2011), which required companies to prioritise data protection and the handling of personal information, but these laws were not designed for today's data-driven decision-making. There was an urgent need for a dedicated legal framework for privacy protection of data in India. In

[1] Yogeshwor Babu Hada,Sai Dhushyanth,Nidhin Mohan,Yahya Hatim,Thilak Raj M,Dr.Kalyana Saravanan, "Analyzing Data Piracy: Causes, Consequences, and Solutions for Enhanced Security in the Digital Age," 11 IJIRT 4222 (2025).

response to this need, the Digital Personal Data Protection Act of 2023 was introduced. The DPDP Act represents a significant milestone in securing India's digital future, ensuring that privacy is recognised as a guaranteed right rather than a privilege. It is India's first comprehensive data protection law aimed at safeguarding citizens' personal data. This law is rooted in the landmark judgment of Justice K.S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors. (2017), which established privacy as a fundamental right. Despite the existence of comprehensive intellectual property laws and cybercrime regulations, digital piracy continues to flourish.[2]

REVIEW OF LITERATURE

Data piracy remains a contested topic as scholars, researchers, and policymakers worldwide have examined data piracy and its enforcement, giving a spectrum of perspectives. A study titled "Data Piracy Laws in India: an in-depth analysis" by Sohan Bhaskar Gawade explains that in this day, where data is often referred to as the "new oil," the increasing threats of data breaches, cyber espionage, and unauthorised exploitation of personal and confidential information require a strong legal mechanism to deal with the above matter. In 2024, Sreevalli Seetharamu, Lakshmi Manasa CN, Anisha Bhattacharya and Dr Chitra BT published research titled "Digital Data Protection Laws: A Review" and examined that the DPDP Bill reflects India's unique socio-economic context and digital landscape. It emphasises free, informed consent, upholds data principals' rights, and places obligations on data fiduciaries regarding data security and transparency. This approach aims to strike a balance between protecting privacy and promoting data-driven innovation, ensuring that India's data protection regime is both comprehensive and adaptable to global standards. They also highlighted that although India is making significant strides in the direction of safety for privacy. Challenges remain in broad government exemptions, unclear cross-border transfer rules, and the absence of a robust, independent data protection authority. One of the articles on the site Vikaspedia, named "Data Protection Laws in India" by Ajay Gautam, explained that the Digital Personal Data Protection Act, 2023, represents a transformative shift in India's legal landscape. It converts privacy from a constitutional principle into an enforceable statutory right, introduces accountability for data-driven businesses, and establishes regulatory oversight in the digital economy. A study by Alok Kumar Singh titled "Data

[2] Dr. Akhilesh Yadav, Mr. Arjun, Mr. Nishant Kumar, "Digital Piracy: Enforcement Challenges under Cyber and IPR Laws," 28 IOSR-JBM 51 (2025).

protection laws in India- an analysis" suggests that, as data protection is one of the most apprehensive topics of discussion in the modern world, the Indian Legislature is, therefore, required to frame more rigid & exhaustive laws for data protection, which require qualitative efforts rather than quantitative.

RESEARCH METHODOLOGY

The research methodology for the analysis of data piracy and its enforcement mechanism in India typically involves a doctrinal and comparative approach. The paper is analytical, explanatory and comparative in nature. The research includes in-depth analyses of:

Primary Sources, including the Indian Constitution, statutory laws, landmark judicial decisions, declarations and other documents on the subject.

Secondary Sources, including journals, research papers, articles, blogs and reports on the issue.

CURRENT LEGAL FRAMEWORK GOVERNING DATA PIRACY IN INDIA

Information Technology Act, 2000, and its Amendments

The Information Technology Act, 2000 (IT Act) is a legislation that grants legal recognition to transactions conducted by electronic data exchange and other forms of electronic communication, popularly known as electronic commerce.[3]

Section 43 of the Information Technology Act (ITA)[4] states that if a person harms the security and integrity of the digital system shall be liable for punishment and compensation to the victim. It also states that if anyone unauthorisedly accesses, downloads, copies, or extracts Data from a computer system without authorisation shall be held liable.

Section 43A of the Act provides that anybody corporate that possesses, deals or handles any "sensitive personal data" or information should maintain reasonable security practices and

[3] Akansh Patel and Piyush Kumar Trivedi, "Security of data piracy: A critical examination of India's intellectual property rights in cyberspace," 10 Int.j.law. 60 (2025).
[4] The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009(India).

procedures relating to such data. It will be liable to pay compensation to the affected person in case of any negligence.[5]

Section 66 of the Act criminalises acts such as hacking, unauthorised access, data theft, introducing malware, etc., mentioned under section 43 without permission with a malicious intention and imposes punishment of imprisonment up to three years, fine up to five lakh rupees, or both.

Under **Section 79** of the IT Act, Platforms (like Telegram, WhatsApp, ISPs, or social media sites) generally enjoy, "meaning they are not legally responsible for that user's post. However, if they fail to take down pirated content after receiving a lawful court order or government notice, they lose this immunity and can be prosecuted as co-conspirators in the piracy.[6]

IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules 2011)

- The IT Rules 2011 (SPDI Rules)[7] describes sensitive personal data, such as financial, health, and biometric information.
- The rules also require the body corporates to be concerned about the data protection or handling of personal data.

Digital Personal Data Protection Act, 2023

The rapid development of technology and widespread use of the internet have drastically transformed how data is collected, stored, and utilised.[8] As technology progressed, the need for stronger regulations became clear. In response, the General Data Protection Regulation (GDPR) was introduced in 2016 to create consistent data protection rules across the EU. The GDPR provided people with better privacy rights, including the ability to access, change, and delete their personal data. The GDPR also influenced countries outside of Europe; it urged nations worldwide to reevaluate and improve their data protection laws.

The need for stronger data protection became necessary in India, following the Supreme Court's historic 2017 judgement (the Puttaswamy judgement) that acknowledged privacy as a

[5] Alaknanda Duggirala, "Data Privacy Protection in India – Technology Vis-à-vis Law," https://www.dlapiperdataprotection.com/?t=law&c=IN (accessed on April 8, 2026).
[6] Drishti IAS, "Digital Piracy in India," https://www.drishtiias.com/daily-updates/daily-news-analysis/digital-piracy-in-india (accessed on 21 May, 2026).
[7] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec.3(i) (Apr. 11, 2011) (India).
[8] Sreevalli Seetharamu, " Digital Data Protection Laws: A Review," 11 Int J Sci Res Sci Eng Technol 65 (2024).

fundamental right. As a result of this judgment, the Justice B.N. Shrikrishna Committee was established to examine the international norms, such as the GDPR and draft India's data protection legislation. Hence, the Digital Personal Data Protection Bill, 2018 was introduced in India.

The version of the DPDP Bill which was eventually passed by both houses of the Indian Parliament marked a few significant changes to the original draft of the DPDP Bill. On August 11, 2023, the Government of India published that version as the Digital Personal Data Protection Act, 2023 (DPDP Act)[9] which will form the personal data protection and regulatory regime in India. The DPDP Act introduces several compliances with respect to the collection, processing, storage and transfer of digital personal data. On November 13, 2025, the Ministry of Electronics and Information Technology (MeitY), notified the DPDP Act and the Digital Personal Data Protection Rules, 2025 (DPDP Rules).[10] The Act will be enforced under the supervision of the Data Protection Board (DPB) and the Telecom Disputes Settlement and Appellate Tribunal will act as the appellate authority. The Digital Personal Data Protection Act 2023 focuses on a consent-first approach, which means data can't be processed without the consent of the individual. Under this act, for the first time in India, the Data Principal is made the centre point of the data ecosystem. The DPDP Act applies to all digital personal data, regardless of whether the data was collected directly in digital form or collected online and subsequently digitised.The DPDP Act provides a legal framework for safeguarding digital personal data particularly relevant in an age where piracy often involves the unauthorized use, sharing, or monetization of individuals' personal and copyrighted content.[11]

Loopholes in Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, is a significant step towards safeguarding the data of Indian citizens. Key features include provisions to protect children's data through mandatory parental control and monitoring. The penalties imposed for violation of the Act along with restrictions on companies that do not comply with the rules, will create greater

[9] The Digital Personal Data Protection Act, 2023, No. 22, Act of Parliament, 2023 (India).
[10] Sajai Singh, "Data Protection Laws of the World," https://www.dlapiperdataprotection.com/?t=law&c=IN (accessed on 6 April, 2026)
[11] *Anand Patel*, "Modern Ipr Piracy In The DigitaliZed Pivotal Era: Indian Law And Global Trends" https://solomonco.in/modern-ipr-piracy-in-the-digitalized-pivotal-era-indian-law-and-global-trends/ (accessed on 21 May, 2026)

accountability for data leaks. However, the Act also has certain loopholes that need the attention of the legislature.[12]

INAPPROPRIATE HANDLING OF SENSITIVE DATA - the Act doesn't hold the Data fiduciary and Data processor (who collect and process data) responsible. Under the Act, the data can only be collected with the consent of the individual. Still, it doesn't say anything about sensitive data such as medical history or sexual orientation, which may cause harm to persons if they are misused.

CERTAIN FIDUCIARIES ARE EXEMPTED - Section 3(c) is not applicable on data collected for personal or domestic use, or for their work as a journalist or artist. This leaves a significant loophole, since even data collected for personal use could be leaked, causing a threat to an individual's privacy.

GOVERNMENT OVERREACH - Section 17 of the Act provides the government with an extensive amount of power by granting it overreaching powers through different exemptions. For example, the Act does not require the government to follow the rules for data principals and data processors if doing so is necessary for reasons of sovereignty, foreign relations, public order, research, archives, etc.

CAPTIVE DATA PROTECTION BOARD - Sections 18 and 19 of the Act establish a Data Protection Board of India to handle grievances. Section 39 states that the court is forbidden to hear or issue injunctions regarding matters that are within the board's jurisdiction. Section 36 additionally provides the government with the power to ask the board for information at any time, if necessary.

Existing structural independence is not stronger than in less developed systems. Appointment, terms of employment, composition, staffing, and most procedural frameworks are under considerable Central Government control.That is particularly troubling in an area in which the State is one of the largest and most significant personal data processors. A privacy framework that applies to the public and private spheres must have a regulator that is not only operationally functional but independent in appearance.[13]

[12] Saloni Chhaparia, “Partial Protection of Privacy is No Protection at all – Lacunae in DPDP Act,” https://www.ispp.org.in/partial-protection-of-privacy-lacunae-in-dpdp-act/ (accessed on 7 April).
[13] Akshita Singh, "Constitutional Status of Data Protection in India: A Critical Analysis of Digital Personal Data Protection Act, 2023,” 8 IJLLR 4646 (2026).

CONSTITUTIONAL ASPECTS AND FUNDAMENTAL RIGHTS

The Indian Constitution does have some provisions like, "Freedom of Speech & Expression & Right to Life & Personal Liberty. The provision had its effects on the right to privacy as the Fundamental Right. There are various cases which do establish the right to privacy as the fundamental right. This proposition was also connected with the new dimension of the Protection of Data. The Link between Data protection & privacy are interdependent on each other. The right to the protection of data is too closely connected with the information of individuals.[14]

Article 19(1)(a) of the Indian Constitution guarantees freedom of speech and expression, which also includes the right to access information, but it must align with the privacy of individuals. Both government agencies and private companies must ensure that personal data and information must not be misused under the pretext of freedom of speech.

Article 19(2) allows the government to put reasonable restrictions on freedom of speech and expression, particularly in matters related to national security, public order, and

defamation. This article becomes critical in controlling digital control, prohibition on spreading of misinformation, and ensuring that confidential information, as well as sensitive data is not misused to incite violence or harm national interest.[15]

JUDICIAL PRECEDENTS

Over the past years, the Indian court has played a crucial role in shaping the legal framework for data protection and strengthening laws related to Data security through various landmark judgments.

Shreya Singhal v. Union of India[16]

In this important decision, the Supreme Court struck down Section 66A of the Information Technology Act, 2000. The Court stated that the section violated Article 19(1)(a) [freedom of speech] and could not be justified under Article 19(2) [reasonable restrictions] of the Indian

[14] Alok Kumar Singh, "Data Protection Laws in India – An Analysis," 6 IJLLR. 5594 (2024).
[15] Sohan Bhaskar Gawade, "Data Piracy Laws in India – An In-depth Analysis" 4 JLRJS. 205 (2025).
[16] Shreya Singal vs. Union of India, AIR 2015 SC 1523

Constitution. The ruling found Section 66A to be too vague and broad to be constitutional. Terms in the section, like "grossly offensive," "menacing," or "annoyance," were unclear and could be misused. This decision highlighted the need for reasonable laws about online content, whether related to data security or social discussions. The case firmly established that while freedom of speech on the internet is vital, it must be balanced with reasonable limits

Justice K.S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors.[17]

On August 24, 2017, the Supreme Court of India declared that the right to privacy is a fundamental right under Article 21 of the Constitution of India. This landmark case challenged the Aadhaar scheme, arguing that it infringed on individuals' privacy rights. The Court's central question was whether the right to privacy falls under the right to life and personal liberty, as defined by Article 21. The ruling affirmed that privacy is an inherent right necessary for the dignity of the individual and is thus protected under Article 21. This decision was crucial in establishing the importance of privacy in a digital age, particularly as personal data such as biometric information can be misused.

This judgement marked a decisive shift in Indian constitutional jurisprudence, establishing informational privacy as an essential facet of dignity, liberty, and autonomy under Articles 14, 19, and 21. In response, the DPDP Act seeks to provide a statutory framework governing the processing of digital personal data.[18]

COMPARISON WITH GLOBAL STANDARDS

The Digital Personal Data Protection Act of 2023 takes inspiration from international standards such as the General Data Protection Regulation (GDPR). However, it differs in key areas. This difference reflects India's unique digital environment and its particular national issues.

The DPDPA of India evidenced a high focus on data sovereignty, where data is required to be localized, and the government is granted a wide-ranging regulatory and enforcement authority. This emphasis reflects the national will to impose national jurisdiction upon personal data, to protect economic interests and to provide more security, which coincides

[17] Justice K.S. Puttaswamy (Retd.) vs. Union of India, AIR 2017 SC (CIV) 2714.
[18] Akshita Singh, "Constitutional Status of Data Protection in India: A Critical Analysis of Digital Personal Data Protection Act, 2023," 8 IJLLR 4620 (2026).

with the constitutional framework putting privacy as one of the fundamental rights of the country but weighing it against the interests of the state as a whole. On the other hand, GDPR focuses on the basic right to data protection in the context of a harmonized, extra-territorial environment. It supports the free movement of data inside and outside the EU that is organized on the basis of rigid provisions of individual rights, transparency, and accountability that aim at empowering individuals and limiting governmental overreach.[19]

India should try to find a balanced approach. Instead of imposing very strict rules, it should protect national interests while also allowing businesses to operate smoothly in the global digital market. This idea is also supported by India's Data Empowerment and Protection Architecture, which focuses on using data in a way that benefits both individuals and businesses.[20]

Another important law is the United States Millennium Copyright Act (DMCA), which provides measures to prevent digital piracy and copyright infringement. India's copyright Act has been amended to adopt some provisions of DMCA which ensure stronger legal protection for intellectual property in this present digital world.[21]

Examining India's legal framework for combating internet piracy reveals a complex environment with changing laws, historical precedents, and enduring difficulties.[22] Evolution of India's data protection regime from fragmented laws like the Information Technology Act, 2000 and SPDI Rules, 2011, towards a unified legislation (Digital Personal Data Protection Act, 2023) has strengthened the data privacy rights in India, but its effectiveness will depend upon how the loopholes of the Act are addressed. After comparison with GDPR, it is observed that the Acts framework is less rights-intensive. Its weakness lies in low literacy rates, lack of public awareness, wide government exemptions and limited independence of the Data Protection Board. Reforms like institutional independence, narrowing the scope of government exemptions, public-facing awareness campaigns, and enabling decentralised or state-level boards are necessary to close the enforcement gaps.

[19] Ashutosh Panda, Dr Amit Kashyap, "Data Sovereignty vs. Data Protection: A Comparative Analysis of India's Privacy Laws and GDPR," 7 IJLLR 8402 (2025).
[20] Priyadharsani Indra R, "Data Protection and Cross-Border Data Transfer," 8 IJLLR 2493 (2026).
[21] Sohan Bhaskar Gawade, "Data Piracy Laws in India – An In-depth Analysis" 4 JLRJS. 206 (2025).
[22] Abhinendra Singh and Mr. Sagar, "The Legal Framework for Combating Online Piracy in India." 8 IJLMH 5740 (2025).

CONCLUSION AND SUGGESTIONS

Data piracy has become a major challenge for India; it is a crime against domestic as well as international law. Rapid digital development has also led to an increase in crimes on the internet. . The borderless nature of the internet, the ease of duplicating and distributing digital content, anonymity tools, and the proliferation of decentralized platforms make detection, attribution, and prosecution of digital piracy extremely difficult.[23]

The law should support the smooth flow of data for business and innovation. Privacy should not be treated as something optional. People should not have to give up their privacy just to use digital services.[24]

The Information Technology Act, 2000, its amendments, the SPDI Rules, 2011, and the Copyright Act, 1957 set the groundwork for regulating digital data in India. However, these laws were not enough to address the challenges of today's data-driven, interconnected economy. As a result, the Digital Personal Data Protection Act, 2023, was introduced, making data privacy a right for everyone, not just a privilege. The Digital Personal Data Protection Act, 2023, represents a step forward in legalising data protection; however, it falls short in adequately guaranteeing the right to privacy.[25]

The DPDP Act aligns with global standards like GDPR, but there are still gaps, including government overreach, improper handling of sensitive data, exemptions for certain data fiduciaries, and limited independence of the Data Protection Board, which requires further improvement. Major court rulings like Shreya Singhal v. Union of India (2015) and Justice K.S. Puttaswamy v. Union of India (2017) have emphasised the constitutional importance of privacy and freedom of speech. These rulings help ensure that laws are in line with fundamental rights.

When comparing with the international standard of GDPR, it is clear that India's DPDP Act follows a model centred on the state. It focuses on sovereignty and national security. In contrast, GDPR emphasises individual empowerment, transparency, and accountability. The study indicates that India has made significant progress in establishing a strong data

[23] Dr. Akhilesh Yadav, Mr. Arjun, Mr. Nishant Kumar, "Digital Piracy: Enforcement Challenges under Cyber and IPR Laws," 28 IOSR-JBM 54 (2025).
[24] Priyadharsani Indra R, "Data Protection and Cross-Border Data Transfer," 8 IJLLR 2504 (2026).
[25] Saloni Chhaparia, "Partial Protection of Privacy is No Protection at all – Lacunae in DPDP Act," https://www.ispp.org.in/partial-protection-of-privacy-lacunae-in-dpdp-act/ (accessed on 21 May, 2026)

protection framework. Nonetheless, the success of the DPDP Act will rely on clear enforcement, the independence of the Data Protection Board, stronger protections for cross-border data transfers, and addressing legislative gaps. Raising awareness and education campaigns about data rights and responsibilities may help the public better comply with the law.