
ALGORITHMIC GOVERNANCE: A COMPARATIVE STUDY OF INDIA'S AND CHINA'S REGULATION OF SOCIAL MEDIA AND DIGITAL PLATFORMS

***Tanya Kaushal**

Student LL.M. (Master of Laws), Amity Institute of Advanced Legal Studies, Amity
University, Noida, Uttar Pradesh, India.

Article Received: 13 September 2026

Article Revised: 03 October 2026

Published on: 23 October 2026

***Corresponding Author: Tanya Kaushal**

Student LL.M. (Master of Laws), Amity Institute of Advanced Legal Studies,
Amity University, Noida, Uttar Pradesh, India.

DOI: <https://doi-doi.org/101555/ijrpa.4129>

ABSTRACT

Social media's and digital platforms' explosive growth has completely changed how people communicate, get information, and engage in public conversation. These platforms are powered by increasingly complex analytic systems that decide what data is shown, suggested, rated, filtered, and prioritised. Because of this, algorithms are much more than just technical tools; they have an increasing impact on how people exercise their rights and how digital society operates.

The regulation of algorithmic governance in China and India is compared in this article, with a focus on social media and digital platforms. The Information Technology Act of 2000, the Information Technology Rules of 2021, the Digital Personal Data Protection Act of 2023, and the Digital Personal Data Protection Rules of 2025 have all contributed to the development of India's regulatory framework. By way of the Internet Information Service Algorithm Recommendation Management Provisions, 2022, the Personal Information Protection Law, 2021, and the Data Security Law, 2021, China, on the other hand, has enacted more precise algorithm-orientated legislation.

With a focus on privacy, accountability, transparency, user autonomy, freedom of expression, and regulatory oversight, the study employs a doctrinal and comparative approach to analyse the two regulatory regimes. It contends that although India's system has a solid constitutional basis, it is nevertheless disjointed from the standpoint of algorithmic accountability. With regard to algorithm review, user choice, algorithm filing, and security assessment, China's

structure offers more direct oversight of algorithmic recommendation services. However, the two nations function in quite distinct institutional and constitutional contexts.

By creating risk-based algorithmic regulation, algorithmic impact assessments, meaningful transparency, user-choice mechanisms, and independent auditing—all while making sure that such regulation stays in line with constitutional rights and judicial review—the paper suggests that India can selectively learn from China's experience.

KEYWORDS: Algorithmic Governance, Social Media, Digital Platforms, Artificial Intelligence, Data Protection, Privacy, Constitutional Rights.

1. INTRODUCTION

Digital platforms are becoming an essential component of modern political, social, and economic life. People's communication and information consumption are influenced by social media platforms, search engines, online markets, and video-sharing services. An individual user's experience is increasingly influenced by algorithmic algorithms that determine whether content is suggested, sorted, or shown in addition to the content submitted by other users.

An important legal challenge is brought up by the increasing use of such systems: who should be held responsible when an algorithm impacts information access or individual rights?

Algorithms are made to work with specific datasets and accomplish specific goals. As a result, its implementation and design may have an impact on freedom of expression, equality, privacy, and consumer autonomy. While profiling systems can deduce a person's interests, preferences, and behavioural traits, recommendation systems might decide what information is displayed. As a result, algorithmic governance is no longer just a technical problem but also a matter of constitutional governance and legal accountability.

The Supreme Court's affirmation of privacy as a basic right made the constitutional significance of digital technology in India especially evident. The Court linked privacy to individual autonomy, liberty, and dignity in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹ These constitutional principles directly relate to algorithmic systems that gather, examine, and use personal data.

Particularly helpful jurisdictions for comparative research are China and India. Both have substantial social media ecosystems and sizable digital populations. Additionally, both have passed laws pertaining to platform duty, cybersecurity, and personal data. However, their methods of algorithmic regulation have evolved in distinct ways.

¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Through a combination of constitutional rights, laws, subordinate laws, and court rulings, India has largely governed internet platforms. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, place extra requirements on intermediaries, while the Information Technology Act, 2000, establishes the fundamental legal framework. India's data protection framework has been further strengthened by the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025.²

Regarding algorithmic systems, China has taken a more direct regulatory stance. Algorithm recommendation services, such as personalised suggestion, ranking, search and filtering, generation and synthesis, scheduling, and decision-making, are particularly governed by its Internet Information Service Algorithm Recommendation Management Provisions, 2022.³

Because it illustrates two distinct approaches to algorithmic governance, the comparison is important. China's system mostly depends on direct administrative regulation and regulatory monitoring, whereas India's framework is substantially affected by judicial review and constitutional rights.

In order to determine if India's current framework adequately handles algorithmic risks and what regulatory lessons might be learned from China's experience without jeopardising constitutional rights, this study looks at various options.

2. STATEMENT OF THE PROBLEM

The lack of a unified, all-encompassing, and algorithm-specific framework regulating the usage of algorithms by social media and digital platforms in India is the main issue this study attempts to address.

A number of elements of the digital ecosystem are governed by Indian law, including cybersecurity, online content, intermediaries, and personal data. However, there isn't a single, all-encompassing legal framework that governs the design, implementation, testing, monitoring, and auditing of algorithmic systems.

This raises a number of legal issues. Users might not understand why specific information is suggested to them. Results from algorithmic profiling could be discriminatory or erroneous.

² *The Information Technology Act, 2000 (Act 21 of 2000); The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; The Digital Personal Data Protection Act, 2023 (Act 22 of 2023); The Digital Personal Data Protection Rules, 2025.*

³ *Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration for Market Regulation, Internet Information Service Algorithm Recommendation Management Provisions, 2022, art. 2.*

Platforms may exploit behavioural data to sway user decisions, and authorities may have trouble assigning blame when an automated system has negative effects.

China has implemented certain algorithmic laws in response to some of these issues. Its model, however, also functions inside a different institutional framework, which raises issues with freedom of speech, administrative control, and the balance between individual autonomy and state oversight.

Therefore, the study investigates whether India needs more precise algorithmic accountability mechanisms and, if yes, what kind of legislation should be implemented within India's constitutional framework.

3. RESEARCH QUESTIONS

1. How do India and China regulate algorithmic governance in relation to social media and digital platforms?
2. What are the principal similarities and differences between the Indian and Chinese regulatory frameworks?
3. To what extent do the two frameworks address privacy, transparency, accountability, freedom of expression, and user autonomy?
4. What regulatory lessons can India draw from China's experience while maintaining constitutional safeguards?

4. RESEARCH OBJECTIVES

The objectives of the research are

1. To examine the legal and regulatory frameworks governing algorithmic systems and digital platforms in India and China.
2. To analyse the constitutional principles relevant to algorithmic governance in India.
3. To examine China's algorithm-specific regulatory mechanisms.
4. To compare the two systems with particular reference to privacy, transparency, user choice, security, and accountability.
5. To identify gaps within India's existing framework and suggest measures for strengthening algorithmic accountability.

5. RESEARCH METHODOLOGY

A doctrinal and comparative legal technique is used in the study. The Indian Constitution, the Information Technology Act of 2000, the Information Technology Rules of 2021, the Digital Personal Data Protection Act of 2023, the Digital Personal Data Protection Rules of 2025,

pertinent Chinese laws and administrative regulations, and court rulings are examples of primary sources.

Books, journal articles, research papers, and academic opinions on algorithmic governance, data security, and digital platform legislation are examples of secondary sources.

The comparative approach is utilised to assess the degree to which particular regulatory processes may be pertinent to India's legal system as well as to find parallels and contrasts between China and India.

An empirical survey is not used in the research. With special emphasis on laws, rules, and judicial interpretation, its main focus is legal and doctrinal.

6. RESEARCH HYPOTHESIS

The study is predicated on the idea that although India has a significant constitutional basis for regulating digital platforms, it does not yet offer an adequate framework for algorithm-specific responsibility. The benefits of direct algorithmic obligations, user-choice mechanisms, risk-based monitoring, and algorithm filing are demonstrated by China's regulatory regime. However, India's constitutional system cannot simply adopt its regulatory framework.

A more equitable type of algorithmic governance might be offered by a rights-based Indian framework that includes algorithmic transparency, impact assessment, independent auditing, and practical remedies.

7. ALGORITHMIC GOVERNANCE IN INDIA

7.1 Constitutional Foundations

There isn't currently a single complete statute in India that governs algorithmic governance. Rather, many facets of algorithmic activity are handled by data protection laws, intermediary regulations, information technology laws, and constitutional measures.

The Constitution's Article 19(1)(a) guarantees the right to free speech and expression. Social media sites are now crucial venues for exercising this freedom in the digital world. In addition to protecting life and individual liberty, Article 21 has been read broadly to encompass privacy.⁴

The ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India* by the Supreme Court is especially noteworthy. The Court acknowledged privacy as a basic right and linked it to

⁴ *The Constitution of India, arts. 19(1)(a) and 21.*

liberty, autonomy, and dignity.⁵ Therefore, algorithmic systems that gather, examine, or deduce personal data function within a constitutional framework where privacy and individual autonomy are crucial.

Digital legislation must, however, take into consideration the state's legitimate interests in upholding cybersecurity, public order, and stopping illegal behaviour. As a result, the legal problem is to strike a balance between conflicting interests using methods that are allowed by the constitution.

7.2 Information Technology Act, 2000

One of the key laws controlling India's digital landscape is still the Information Technology Act of 2000.

Intermediaries are granted a conditional exemption from responsibility under Section 79, subject to certain criteria and due diligence obligations.⁶ A statutory tool for preventing public access to information under certain conditions is provided under Section 69A.⁷

Even though algorithmic recommendation systems are not expressly regulated by the Information Technology Act, these laws are now pertinent to the larger regulation of digital platforms.

In *Shreya Singhal v. Union of India*, the constitutional restrictions on digital control were made much clearer. Section 66A of the Information Technology Act was overturned by the Supreme Court on the grounds that it violated Article 19(1)(a) by restricting online communication.⁸

Shreya Singhal's significance goes beyond section 66A. It shows that constitutional restrictions on the right to free speech and expression nevertheless apply to the control of online platforms and digital technology.

7.3 Information Technology Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, added new requirements for major social media intermediaries and increased intermediary due diligence standards.⁹

The rules impose different compliance duties on intermediaries and mandate grievance redressal systems. The rising use of automated methods by social media platforms for content

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁶ *The Information Technology Act, 2000 (Act 21 of 2000)*, s. 79.

⁷ *Id.*, s. 69A.

⁸ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁹ *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

moderation, recommendation, and ranking makes these provisions pertinent to algorithmic governance.

However, the rules were not intended to provide a complete foundation for algorithmic responsibility. Instead of creating specific requirements for algorithmic effect assessments, independent algorithm audits, or explainability, they mostly concentrate on intermediary accountability, content governance, and compliance.

This distinction is crucial. Even if a platform complies with intermediary duties, consumers and regulators may still find it challenging to comprehend the algorithm that determines content visibility.

Since then, MeitY has taken into account changes pertaining to artificially generated data. Instead of presenting them as a distinct announced 2026 algorithmic-governance statute, MeitY's public material refers to these as draft modifications and consultation material.¹⁰

7.4 Digital Personal Data Protection Framework

A legal foundation for processing digital personal data is provided by the Digital Personal Data Protection Act, 2023, which also lays out requirements for data fiduciaries' and data principals' rights.¹¹

On November 14, 2025, the Ministry of Electronics and Information Technology announced the Digital Personal Data Protection Rules, 2025, which offer comprehensive implementation procedures under the Act.¹²

Since many algorithmic systems employ personal data for prediction, recommendation, and profiling, the framework is intimately related to algorithmic governance.

But algorithmic responsibility and data protection are not the same. An algorithm may produce erroneous, discriminatory, or otherwise detrimental results even in cases when personal data is treated legally.

As a result, while India's data-protection framework covers a significant aspect of algorithmic governance, it does not control every step of the algorithmic lifecycle, including design, training, deployment, monitoring, auditing, and challenge.

¹⁰ Ministry of Electronics and Information Technology, Government of India, "Draft Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 relating to Synthetically Generated Information" (October 22, 2025), available at: <https://www.meity.gov.in/> (last visited on September 28, 2026).

¹¹ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

¹² Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025 (November 14, 2025), available at: <https://www.meity.gov.in/> (last visited on September 28, 2026).

8. ALGORITHMIC GOVERNANCE IN CHINA

8.1 Personal Information Protection Law

A thorough framework for the processing of personal data is provided under China's Personal Information Protection Law, 2021. It offers further protections for sensitive personal data and lays down guidelines and responsibilities for those who process personal data.¹³

Because algorithmic systems routinely employ personal data for automated analysis, recommendation, and profiling, the law is pertinent to algorithmic governance.

China's Data Security Law, 2021, provides the broader regulatory framework that digital platforms operate under and is a component of the larger legal framework managing data security.¹⁴

8.2 Algorithm Recommendation Management Provisions, 2022

The Internet Information Service Algorithm Recommendation Management Provisions, 2022, is China's most important algorithm-specific legislative development.

In addition to identifying technologies like personalised recommendation, ranking and selection, search and filtering, generation and synthesis, and scheduling and decision-making, the provisions also apply to algorithm recommendation services.¹⁵

This strategy is important because, instead of being regulated only indirectly through data protection or intermediary liability, algorithms themselves become a specific regulatory object.

The provisions mandate that algorithm recommendation service providers set up procedures for reviewing algorithm mechanisms, protecting personal information, data security, scientific and technology ethics, security monitoring, and emergency response.¹⁶

Providers must also periodically review, evaluate, and verify algorithm mechanisms, models, data, and application results.¹⁷

A comparatively straightforward method of algorithmic accountability is represented by these clauses.

8.3 Transparency and User Choice

In addition to identifying technologies like personalised recommendation, ranking and selection, search and filtering, generation and synthesis, and scheduling and decision-making, the provisions also apply to algorithm recommendation services.

¹³ *Personal Information Protection Law of the People's Republic of China, 2021, arts. 1–13.*

¹⁴ *Data Security Law of the People's Republic of China, 2021.*

¹⁵ *Cyberspace Administration of China et al., Internet Information Service Algorithm Recommendation Management Provisions, 2022, art. 2.*

¹⁶ *Id.*, art. 7.

¹⁷ *Id.*, art. 8.

This strategy is important because, instead of being regulated only indirectly through data protection or intermediary liability, algorithms themselves become a specific regulatory object.

The provisions mandate that algorithm recommendation service providers set up procedures for reviewing algorithm mechanisms, protecting personal information, data security, scientific and technology ethics, security monitoring, and emergency response.

User rights are another significant aspect of the Chinese framework.

Algorithm recommendation service providers are required by the provisions to safeguard users' algorithmic awareness and choice. The provision of algorithm recommendation services as well as the fundamental ideas, goals, and main working mechanisms of the pertinent services must be explained to users.¹⁸

Additionally, the regulatory framework mandates that providers give consumers accessible ways to disable algorithm recommendation services or options that are not based on personal attributes.¹⁹

In terms of algorithmic recommendation, this is an explicit legislative approach to user autonomy.

The laws also govern how user models and user tags are managed, requiring providers to provide suitable guidelines for the traits and interests included in user profiles.²⁰

8.4 Algorithm Filing and Regulatory Supervision

An algorithm-filing system has also been created in China.

Algorithm filing must be completed through the specified system by algorithm recommendation service providers with public opinion attributes or social mobilisation skills.²¹

Additionally, the regulatory framework offers supervisory inspection and security evaluation. In addition to keeping pertinent network logs, providers must assist regulatory bodies with security evaluations and oversight.²²

As a result, the Chinese approach goes beyond just mandating that businesses adhere to broad data-protection standards and establishes particular regulatory measures aimed against algorithmic systems.

¹⁸ *Id.*, art. 16.

¹⁹ *Id.*, art. 17.

²⁰ *Id.*, art. 10.

²¹ *Id.*, art. 24.

²² *Id.*, arts. 27–28.

9. COMPARATIVE ANALYSIS OF INDIA AND CHINA

9.1 Regulatory Structure

The structure of regulation is the first significant distinction.

Constitutional provisions, laws, subordinate laws, and court rulings make up India's framework. Therefore, rather than originating from a single algorithmic statute, algorithmic governance arises from multiple areas of law.

In response to algorithmic recommendation systems, China has enacted particular regulatory regulations. Algorithmic technologies are specifically identified in the 2022 Provisions, which also set providers' obligations.²³

9.2 Algorithmic Specificity

The rules that are now in place in India govern online content, personal data, and intermediaries, but they do not provide a single, all-encompassing framework for algorithmic responsibility.

Algorithmic recommendation systems are directly regulated by China's Algorithm Recommendation Management Provisions, which also mandate that providers do regular reviews and evaluations.²⁴

This distinction highlights the distinction between controlling the platform and controlling the technology that the platform uses to exert its impact.

9.3 User Autonomy

The Chinese architecture specifically gives customers algorithmic choice tools, such as the ability to reject personalised recommendations or disable algorithm recommendation services.²⁵

The privacy and data-protection regime in India offers significant safeguards for consent and personal information, but it lacks a general statutory procedure comparable to China's explicit algorithmic opt-out laws.

9.4 Risk and Regulatory Assessment

Additional legal requirements for algorithm recommendation services with social mobilisation or public opinion features are incorporated into China's system.²⁶

²³ *Cyberspace Administration of China et al., Internet Information Service Algorithm Recommendation Management Provisions, 2022.*

²⁴ *Id.*, art. 8.

²⁵ *Id.*, art. 17.

²⁶ *Id.*, art. 24.

The current Indian framework is more dependent on government directives, judicial scrutiny, intermediary obligations, and data protection regulations. This points to an area where India can think about creating a risk-based strategy that is more structured.

9.5 Constitutional Protection

India's framework functions under a constitutional framework that prioritises equality, freedom of speech, privacy, and judicial review. *Puttaswamy* outlines privacy as a basic right, whereas *Shreya Singhal* illustrates the constitutional bounds on online speech regulation.²⁷

China's framework functions in a distinct constitutional and institutional context, emphasising public order, cybersecurity, administrative supervision, and state regulatory goals.

As a result, India cannot simply adopt China's institutional model, even though its regulatory procedures may offer comparable lessons....

10. CRITICAL ANALYSIS AND ORIGINAL CONTRIBUTION

The comparative research shows that algorithmic governance is more than just a continuation of data protection or content regulation.

Even when the underlying material is legal and the data has been processed in compliance with relevant regulations, an algorithm may have serious repercussions. While profiling systems could create false assumptions about people, recommendation systems might rank material based on engagement-based goals.

Therefore, creating a risk-based strategy should be the first major adjustment.

The level of danger associated with each method varies. A system that makes entertainment material recommendations may not always give rise to the same legal issues as one that affects people's access to jobs, credit, necessary services, or other issues with significant ramifications.

Therefore, India can think about categorising algorithmic systems based on their possible effects. Increased openness, impact assessment, and auditing requirements may apply to higher-risk systems.

Algorithmic impact evaluation is the second prerequisite. Before deploying high-impact algorithmic systems and on a regular basis afterward, providers should evaluate potential effects on security, equality, privacy, discrimination, and other fundamental rights.

Third, real transparency should be encouraged by regulation. Due to cybersecurity and valid business considerations, full disclosure of source code may not always be required or

²⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

suitable. Nonetheless, the main goals, contributing elements, and outcomes of important algorithmic systems should be clear to users and regulators.

Fourth, there should be more user autonomy. People should be able to make meaningful decisions about personalised recommendation systems, especially when there is a lot of profiling. A helpful comparable example is China's explicit acceptance of algorithmic choosing.²⁸

Fifth, accountability could be strengthened by independent auditing. In situations when algorithmic systems have substantial effects on people or society, internal platform evaluations might not always be enough.

However, algorithmic transparency cannot be used as an unqualified defence of legislative restrictions on free speech. Any Indian framework must adhere to the fundamental rights, proportionality, and legality standards found in the constitution.

Therefore, this paper's unique contribution is the suggestion of an algorithmic governance model for India that is both rights-based and risk-sensitive. People should be able to make meaningful decisions about personalised recommendation systems, especially when there is a lot of profiling. A helpful comparable example is China's explicit acceptance of algorithmic choosing.

India could carefully integrate processes like risk classification, algorithmic effect assessment, user choice, and independent audits while integrating them under constitutional protections and judicial scrutiny, as opposed to imitating China's regulatory framework.

Algorithmic explanation and algorithmic disclosure are further distinguished in the paper. Mandatory disclosure of proprietary source code shouldn't always be the goal. Rather, regulations should mandate adequate explanations of how important algorithmic systems function and impact users so that their choices can be comprehended and, if needed, contested.

With this strategy, India would be able to transition from a disjointed platform regulation model to a more unified framework of algorithmic accountability.

²⁸ *Cyberspace Administration of China et al., Internet Information Service Algorithm Recommendation Management Provisions, 2022, art. 17.*

11. FINDINGS

The primary findings are:

In particular, where profiling is intensive, people should be able to take meaningful decisions concerning customised recommendation systems. A useful comparison is China's open acceptance of algorithmic selection.

First, while India has developed a large body of regulation relating to digital platforms, intermediaries and personal data, control of algorithms continues to be scattered across a range of legal systems.

Second, the constitutional concept of India provides a strong base to protect individual liberty, speech and privacy in the digital space.

Third, China has implemented more direct regulation of algorithmic recommendation services with the 2022 Algorithm Recommendation Management Provisions.

Fourth, China's approach demonstrates the regulatory value of algorithmic review, user choice, algorithm filing, and security evaluation.

Fifth, algorithmic governance raises issues that go beyond technology, such as institutional accountability, privacy, equality, autonomy, and freedom of expression.

Sixth, selectively modifying some regulatory systems while making sure they function within India's constitutional framework may be advantageous.

12. RECOMMENDATIONS

12.1 Creating a Framework Based on Risk

People have to be able to make meaningful decisions about personalised recommendation systems, particularly when there's a lot of profiling. A useful parallel is the open embrace of algorithmic selection in China.

India must look about building a legal or regulatory framework that categorises algorithmic systems depending on their potential impacts.

12.2 Evaluations of Algorithmic Impact

Periodic impact evaluations that cover privacy, discrimination, security, accuracy, and consequences for fundamental rights should be conducted on high-risk algorithmic systems.

12.3 Significant Openness

Platforms should provide clear information about the main goals and variables affecting important algorithmic results.

12.4 Choice of the User

When appropriate, users should have meaningful options to limit or disable personalised recommendations.

12.5 Unbiased Evaluation

Periodic independent audits that look at privacy, discrimination, security, and compliance issues should be conducted on high-impact algorithmic systems.

12.6 Workable Solutions

People who are greatly impacted by algorithmic systems should have easy access to grievance procedures and, where necessary, channels for contesting decisions and getting explanations.

12.7 Constitutional Protections

People should be able to make meaningful decisions about personalised recommendation systems, especially when there is a lot of profiling. A helpful comparable example is China's explicit acceptance of algorithmic choosing.

Freedom of speech, privacy, equality, and other fundamental rights should be upheld by any algorithmic regulatory structure. The legality and proportionality requirements of the constitution should continue to govern government intervention.

12.8 Autonomous Supervision

To ensure that the regulatory authority itself is held accountable, algorithmic governance should include independent scrutiny and institutional protections.

13. CONCLUSION

Algorithmic governance has become a major legal concern, as digital platforms gain more and more power through automated systems that select how material is organised, recommended and presented. Algorithms thus influence not only technology processes but also public communication, privacy, autonomy and access to information.

China and India are two quite different regulatory strategies in comparison. India has built its digital architecture in a piecemeal fashion through data protection, intermediary regulation, and constitutional principles. Its key constitutional strength is its guarantee of freedom of expression and privacy. Puttaswamy created the basis for privacy as a fundamental constitutional value, while Shreya Singhal reaffirmed the constitutional protection of online expression.

Conversely, China has opted for direct regulation of specific algorithms. The 2022 Algorithm Recommendation Management Provisions, in addition to regulating recommendation

technology, also set out procedures for algorithm review, algorithm security, user choice, filing and regulatory assessment.

The comparison does not imply that the full regulatory framework of one country can be easily transplanted to another. The institutional and constitutional environment of China and India are very different. But the Chinese example demonstrates the utility of treating algorithms as an object of legal regulation.

Therefore, India could also take further specific regulatory measures in addition to its existing constitutional provisions. risk classification, algorithmic effect assessment, meaningful disclosure, user choice mechanisms and independent audits could bring further accountability.

“We shouldn’t be regulating technology just because it’s technologically advanced. Instead, rules should focus on cases that involve algorithmic systems that have a significant influence on people or society.

India could address algorithmic threats while facilitating technological innovation and constitutional liberties within a rights-based, risk-sensitive and technology neutral framework. Such a paradigm would recognise that the goals of constitutional rights and technical progress are not mutually exclusive.

At the end of the day, the question of how algorithms should be regulated is not the core issue of algorithmic governance. It is about how to know how the law can make sure that technological systems that can potentially impact persons and society are held accountable, transparent, proportionate and constitutional.

BIBLIOGRAPHY

A. BOOKS, JOURNAL ARTICLES, AND RESEARCH MATERIAL

1. Ajay Kumar Bisht and Neeruganti Shanmuka Sreenivasulu, “Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023” (2024).
2. Medha Kolanu, Rudraksh Lakra, and Abhijeet Shrivastava, “Data, Control, and Power: Decoding India’s Digital Personal Data Protection Act, 2023,” 6(4) *Global Privacy Law Review* 136–155 (2025).
3. Sonia Nath and Rumi Dhar, “An Analysis of the Digital Personal Data Protection Act 2023,” 15(1) *Christ University Law Journal* 99–126 (2026).
4. Debapom Purkayastha, *Data Privacy: Fact or Fiction? An Analysis of the Digital Personal Data Protection Act, 2023* (LL.M. Dissertation, National Law University and Judicial Academy, Assam, 2024).

5. Zhaohui Su et al., "China's Algorithmic Regulations: Public-Facing Communication is Needed," 12 *Health Policy and Technology* 100719 (2023).

B. INDIAN STATUTES AND REGULATIONS

6. The Constitution of India, 1950.
7. The Information Technology Act, 2000 (Act 21 of 2000).
8. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
9. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
10. The Digital Personal Data Protection Rules, 2025.

C. CHINESE LAWS AND REGULATIONS

11. *Personal Information Protection Law of the People's Republic of China*, 2021.
12. *Data Security Law of the People's Republic of China*, 2021.
13. *Internet Information Service Algorithm Recommendation Management Provisions*, 2022.

D. CASES

14. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
15. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

E. GOVERNMENT AND INSTITUTIONAL MATERIALS

16. Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Rules*, 2025.
17. Ministry of Electronics and Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021.
18. Ministry of Electronics and Information Technology, Government of India, *Draft Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 relating to Synthetically Generated Information*, 2025.
19. Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and State Administration for Market Regulation, *Internet Information Service Algorithm Recommendation Management Provisions*, 2022.