Rethinking Constitutionalism in the Digital Age Digital Rights, Technology and Global Internet Governance

Name: **Aditya Tripathi** A03104426019
LLM (IP) AMITY LAW SCHOOL
2026-2027

ABSTRACT

The expansion of artificial intelligence, algorithmic decision-making, biometric surveillance, social-media platforms and digital infrastructure has altered the location and exercise of constitutional power. Classical constitutionalism was principally designed to restrain the State through the rule of law, separation of powers, fundamental rights and judicial review. In the digital environment, however, power is increasingly exercised through data systems, algorithms and private platforms as well as traditional public institutions. This paper examines whether classical constitutionalism can adequately respond to these developments or whether a complementary framework of digital constitutionalism is required. It studies privacy, freedom of expression, equality, Internet shutdowns, AI surveillance, platform power and global Internet governance, with particular reference to India. Contemporary examples include the 2026 Jantar Mantar student protests and reported use of AI-assisted facial recognition and targeted Internet restrictions, the 2024 Manipur student protests and Internet suspension, and the 2026 Jharkhand student movement concerning alleged recruitment-examination irregularities. Comparative reference is made to the European Union and United States. The paper argues that digital constitutionalism should not displace classical constitutionalism; rather, it should extend constitutional principles of legality, proportionality, transparency, accountability, equality, privacy, due process and human oversight to digital spaces and technologically mediated public and private power.1

CHAPTER 1: INTRODUCTION

Digital technology has become part of the ordinary exercise of governmental, economic and social power. Public authorities use databases, biometric identification, predictive tools and digital communications systems, while private technology companies determine how information is created, ranked, recommended and removed. Consequently, constitutional law can no longer examine power only through the conventional relationship between the State and the individual.2

Constitutionalism is concerned with the limitation of power. A written Constitution establishes institutions and legal rules, but constitutionalism requires that those institutions actually remain subject to law, rights and accountability. The digital environment creates a new problem because Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar', 24 July 2026.

1.M. P. Jain, Indian Constitutional Law (8th edn., LexisNexis 2018).

important decisions affecting liberty may be produced by systems that are technically complex, privately owned or geographically dispersed.3

The central research problem is therefore whether a constitutional model developed around State power can adequately control algorithmic and platform power. The study asks whether traditional rights such as privacy, equality, speech and due process can be applied to AI surveillance, automated decisions and digital platforms, and whether global Internet governance requires common constitutional principles.4

The paper adopts a doctrinal and comparative methodology. It examines constitutional provisions, statutes, judicial decisions, international and institutional materials, academic literature and recent reports. India is the principal jurisdiction, with comparative reference to the European Union and United States.5

The hypothesis is that classical constitutionalism remains necessary but is not, by itself, institutionally sufficient for the digital age. Digital constitutionalism is required as an extension of existing constitutional values rather than as a

replacement for them.6

CHAPTER 2: THEORETICAL FOUNDATIONS OF CLASSICAL CONSTITUTIONALISM

Constitutionalism is the idea that political power must be limited and exercised according to law. It includes the rule of law, separation of powers, protection of rights, judicial independence and accountability. A Constitution may formally exist without effective constitutionalism; constitutionalism requires the practical acceptance of limits on public power.7

The distinction between Constitution and constitutionalism is particularly important in digital governance. The Constitution provides the legal architecture of the State, whereas constitutionalism supplies the normative demand that power—whether political or technological—remain justified, reviewable and accountable.8

2.H. W. R. Wade and C. F. Forsyth, Administrative Law (11th edn., Oxford University Press 2014).

3.Constitution of India, 1950, arts. 14, 19 and 21.

4.European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act).

5.Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

6.Digital Personal Data Protection Act, 2023.

7.Information Technology Act, 2000.

Liberal constitutionalism emphasises individual liberty and limited government. Republican constitutionalism adds the concern of freedom from domination and meaningful civic participation. Post-colonial constitutionalism, especially in India, places these ideas alongside social justice, equality, dignity and democratic transformation.9

The rule of law requires that governmental action have legal authority and not be arbitrary. This principle is increasingly relevant where authorities deploy facial recognition, predictive policing or automated eligibility systems. Technological capability cannot itself constitute legal authority. The fact that a government possesses a database or AI tool does not mean that it may use it without statutory and constitutional justification.10

Separation of powers also requires adaptation. Automated systems may be designed by executive agencies, supplied by private companies and operated by officials, while judicial review may be the only mechanism through which affected citizens can challenge them. The judiciary therefore remains essential in ensuring that technological governance complies with constitutional standards.11

Fundamental rights and judicial review form the principal bridge between classical and digital constitutionalism. The Indian Supreme Court's privacy jurisprudence demonstrates that constitutional rights can evolve with technology without abandoning their original values.12

CHAPTER 3: THE DIGITAL TRANSFORMATION OF CONSTITUTIONALISM

Technology changes not merely the tools of government but the structure of power itself. A traditional administrative decision may affect a defined group, whereas an algorithm can classify or rank millions of people simultaneously. Data also permits authorities and companies to observe patterns of behaviour that would previously have remained invisible.13

The State is no longer the only significant holder of digital power. Search engines, social-media companies, cloud providers and large platforms control communication infrastructure on which

8.Constitution of India, 1950, arts. 14, 19 and 21.

9.Indian Express, ‘Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar

Mantar', 24 July 2026.

10. Indian Express, 'Mobile internet snapped again around Delhi's Jantar Mantar, 6th such order in a week', 23 July 2026.

11. Internet Society Pulse, 'Cost of Access: When the Internet Goes Dark, People Become the Network', 20 August 2026.

12. Indian Express, 'Manipur on the boil again: Protests after fresh violence, Internet snapped in valley districts', 11 September 2024.

democratic participation increasingly depends. Their terms of service, recommendation systems and content-moderation policies can influence the visibility of political speech.14

Artificial intelligence intensifies these concerns. Algorithms can identify faces, detect patterns, generate content and support decisions. Yet algorithmic systems may be opaque, dependent on biased datasets and difficult for individuals to challenge. A constitutional system cannot permit technical complexity to become a shield against accountability.15

This has produced the idea of digital constitutionalism: the extension of constitutional values to digital environments and new forms of public and private power. Its central principles include privacy, digital liberty, equality, freedom of expression, transparency, accountability, procedural fairness and human oversight.16

Digital constitutionalism should not be understood as a separate Constitution for the Internet. Its purpose is to ensure that the constitutional commitment to limited and accountable power remains meaningful when the method of exercising power changes from an identifiable government order to an algorithm, database or platform rule.17

CHAPTER 4: DIGITAL RIGHTS AND CONSTITUTIONAL PROTECTION

Digital rights are increasingly necessary for effective participation in contemporary society. Privacy is central because digital systems can collect, combine and infer information about individuals. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a fundamental right connected with dignity, liberty and autonomy. Informational privacy is particularly important where governments and companies process large quantities of personal data.18

Freedom of expression also has a digital dimension. In Shreya Singhal v. Union of India, the Supreme Court struck down section 66A of the Information Technology Act, 2000, recognising the danger of vague restrictions on online speech. In Anuradha Bhasin v. Union of India, the Court held

13. India Today, 'Internet suspended in five Manipur districts for 5 days amid student agitation', 10 September 2024.

14. India Today, 'Not going back: Jharkhand aspirants camp in Ranchi over recruitment row', 30 July 2026.

15. Constitution of India, 1950, arts. 14, 19 and 21.

16. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act).

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

that freedom of speech and expression through the Internet is constitutionally protected and subjected restrictions to constitutional scrutiny.19

Equality presents a further challenge. Algorithms may reproduce historical bias in training data and produce discriminatory outcomes while appearing technically neutral. Article 14 therefore has relevance to automated decision-making. A person should not lose a constitutional opportunity merely because discrimination has been hidden inside software.20

Internet access has also become closely connected with education, employment, communication and public participation. Shutdowns can consequently affect several rights simultaneously. The Manipur experience illustrates this problem. During student protests in September 2024, Internet services were suspended in five valley districts

amid concerns over public order and inflammatory material. The restriction affected mobile data as well as other forms of connectivity.21

Digital due process should include notice, reasons, an opportunity to challenge, meaningful human review and an effective remedy. Where an automated system produces a decision with serious consequences, procedural fairness should not disappear merely because the decision was technologically assisted.22

The constitutional protection of digital rights also requires attention to the relationship between privacy and public participation. Privacy is not limited to secrecy. It protects the ability of a person to decide when, how and for what purpose personal information is disclosed. In a democratic society, this matters particularly during political meetings and protests. If attendance at a peaceful gathering can be automatically recorded, identified and linked with other databases, the resulting surveillance may discourage lawful participation even where no arrest takes place. The constitutional injury may therefore arise through a chilling effect rather than through an immediate physical interference with liberty.23

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

19. Constitution of India, 1950, arts. 14, 19 and 21.

20. Indian Express, 'Manipur on the boil again: Protests after fresh violence, Internet snapped in valley districts', 11 September 2024.

21. ICANN, 'About ICANN', official institutional materials.

63. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; see also the discussion of informational privacy and personal liberty therein.

CHAPTER 5: ARTIFICIAL INTELLIGENCE AND CONSTITUTIONAL CHALLENGES

AI creates constitutional questions because it allows decisions to be made or assisted by systems that may not be transparent to affected individuals. AI-based surveillance is particularly sensitive. Facial recognition can identify people in public places and potentially connect their physical presence with government databases.24

The 2026 Jantar Mantar protests in Delhi provide a significant contemporary illustration. During student demonstrations, reports described police surveillance vans using live video and AI-assisted facial recognition. Police stated that the system was intended to identify persons with previous criminal records, while protesters and rights advocates raised concerns about continuous monitoring, privacy and intimidation. A public interest challenge subsequently raised questions concerning the legal and constitutional basis of such surveillance.25

The constitutional concern is not simply whether police can identify a person. It is whether the State has adequate legal authority, whether the surveillance is necessary and proportionate, what data is retained, who can access it, and what remedy exists if the system wrongly identifies an individual. The chilling effect is also relevant: citizens may hesitate to attend a lawful demonstration if they believe their identity will be automatically recorded and analysed.26

AI decision-making creates similar concerns in welfare, recruitment, policing and public administration. The responsible authority cannot shift responsibility to the algorithm. Human institutions must remain answerable for automated outcomes.27

Transparency is therefore essential. Individuals should know what category of data is used, what purpose the system serves, how a decision was reached and how it can be challenged. High-risk systems should undergo impact assessments and independent review.28

The European Union's AI Act demonstrates a risk-based regulatory approach, while India's framework is still developing. Whatever regulatory model is adopted, constitutional principles should remain the baseline for governmental use of AI.29

22. Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar

Mantar', 24 July 2026.

23. Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar', 24 July 2026.

24. Constitution of India, 1950, arts. 14, 19 and 21.

25. M. P. Jain, Indian Constitutional Law (8th edn., LexisNexis 2018).

26. H. W. R. Wade and C. F. Forsyth, Administrative Law (11th edn., Oxford University Press 2014).

A further difficulty is the problem of false positives. Facial recognition and predictive systems operate through probabilities and statistical matching. A person may therefore be incorrectly identified even though the system appears objective. Such errors can be especially serious when an automated match is followed by police questioning, detention or adverse profiling. Constitutional safeguards must consequently operate before, during and after the technological process. Independent testing, accuracy standards, audit trails, deletion procedures and a meaningful mechanism for correcting erroneous identification should form part of any lawful surveillance framework.30

CHAPTER 6: TECHNOLOGY PLATFORMS AND THE CONSTITUTIONALISATION OF PRIVATE POWER

The digital age complicates the assumption that constitutional threats arise only from government. Large technology platforms exercise substantial control over communication, information and public discourse. Their decisions concerning account suspension, recommendation, advertising and content removal can have consequences comparable in social importance to traditional public decisions.31

This does not mean that every private company should automatically be treated as a constitutional State. Private autonomy and editorial freedom remain important. However, when a platform becomes essential to democratic communication, legal systems may legitimately demand transparency, procedural safeguards and accountability.32

Content moderation presents a difficult balance. Insufficient moderation can expose users to threats, incitement and misinformation, while excessive moderation can suppress legitimate political speech. A fair framework should therefore require clear rules, reasons for significant decisions, accessible appeals and transparency reports.33

Platform constitutionalism describes the development of internal rules and procedures within digital platforms that resemble constitutional arrangements: rights, restrictions, adjudication, enforcement

27. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act).

64. European Union, Regulation (EU) 2024/1689, Artificial Intelligence Act.

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

29. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

30. Digital Personal Data Protection Act, 2023.

and appeals. The importance of this concept lies in recognising that private rules can have public consequences.34

A modern constitutional framework should consequently regulate significant private digital power without simply converting private companies into government institutions. The goal should be prevention of arbitrary digital power.35

The problem of private digital power is especially visible where a platform becomes a principal forum for political communication. Traditional constitutional doctrine generally distinguishes State action from private conduct. Yet digital dependence can make that distinction less persuasive from the perspective of practical liberty. The appropriate response is not to impose every constitutional duty directly upon private companies, but to create statutory duties proportionate to their social importance. Large platforms can be required to provide procedural fairness, transparency and remedies while retaining legitimate freedom to organise their services.36

CHAPTER 7: GLOBAL INTERNET GOVERNANCE AND DIGITAL CONSTITUTIONALISM

The Internet is global, but law remains predominantly territorial. This creates a structural tension between national sovereignty and transnational digital activity. A platform may be incorporated in one jurisdiction, process data in another and serve users worldwide.37

Internet governance is therefore distributed among States, international organisations, technical bodies, private companies, civil society and users. ICANN illustrates the multistakeholder model through coordination of the Internet's unique identifier systems. The Internet Governance Forum provides a global forum for policy discussion and cooperation.38

The multistakeholder model is important because no single government can realistically regulate every aspect of the global Internet. At the same time, private actors should not become unaccountable global regulators.39

---

31. Information Technology Act, 2000.

32. Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar', 24 July 2026.

65. Moody v. NetChoice, LLC, 603 U.S. 707 (2024).

33. Indian Express, 'Why police surveillance and facial recognition at Jantar Mantar are under legal challenge', 25 July 2026.

34. ICANN, 'About ICANN', official institutional materials.

35. Internet Society Pulse, 'Cost of Access: When the Internet Goes Dark, People Become the Network', 20 August 2026.

Global digital constitutionalism should establish minimum principles applicable across jurisdictions: privacy, freedom of expression, protection against arbitrary surveillance, transparency in high-risk AI, due process, cybersecurity and access to effective remedies.40

Such a framework need not eliminate national differences. Instead, it should establish a constitutional floor below which digital governance should not fall.41

CHAPTER 8: COMPARATIVE APPROACHES TO DIGITAL CONSTITUTIONALISM

India, the European Union and the United States provide useful comparative models.42

India's constitutional approach relies substantially on Articles 14, 19 and 21. Puttaswamy transformed privacy jurisprudence, while Shreya Singhal and Anuradha Bhasin extended constitutional protection to digital expression and Internet access. India's Digital Personal Data Protection Act, 2023 adds a statutory data-protection framework.43

The European Union adopts a more detailed regulatory approach. The General Data Protection Regulation provides strong data-protection rights, the Digital Services Act regulates online platforms, and the AI Act uses a risk-based framework for artificial intelligence. The EU model demonstrates how fundamental rights can be incorporated into technology regulation through detailed legislation.44

The United States relies heavily on constitutional free-speech protection, particularly the First Amendment, and uses sectoral approaches to privacy. Cases such as Carpenter v. United States demonstrate judicial adaptation of traditional constitutional principles to digital information. Moody
v. NetChoice illustrates the difficulty of regulating private platforms while respecting constitutional protections for editorial discretion.45

India occupies an intermediate position. Its courts have developed broad constitutional principles, while legislation and regulatory mechanisms continue to evolve. The comparative lesson is that judicial review, rights-based

legislation and regulatory institutions must operate together.46

36. Indian Express, 'Manipur on the boil again: Protests after fresh violence, Internet snapped in valley districts', 11 September 2024.

37. India Today, 'Internet suspended in five Manipur districts for 5 days amid student agitation', 10 September 2024.

38. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act).

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

40. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act).

41. Carpenter v. United States, 585 U.S. 296 (2018).

42. European Union, Regulation (EU) 2022/2065 (Digital Services Act).

CHAPTER 9: CONTEMPORARY CHALLENGES AND THE FUTURE OF CONSTITUTIONALISM

The recent protest examples demonstrate why digital constitutionalism is a practical rather than theoretical issue.47

The Jantar Mantar episode combines surveillance and communication restrictions. Reports in July 2026 described AI-assisted facial recognition of protesters and targeted mobile-Internet restrictions around the demonstration site. These developments raise simultaneous questions under privacy, expression and peaceful assembly. They also illustrate how two forms of digital power—surveillance and communication control—can operate together.48

The Manipur student protests show how Internet shutdowns can affect communication during political unrest. Although public order is a legitimate constitutional concern, prolonged or broad shutdowns may affect education, commerce, access to emergency information and democratic participation.49

The 2026 Jharkhand student protests concerning alleged irregularities in JPSC and JSSC recruitment examinations provide a different perspective. Thousands of aspirants protested over alleged examination and recruitment irregularities and demanded accountability. The episode illustrates that digital constitutionalism also includes technological fairness and procedural accountability in public administration. Where recruitment and examination processes depend upon digital registration, data processing and computerised systems, citizens reasonably expect transparent and reviewable procedures.50

Other emerging challenges include deepfakes, AI-generated political misinformation, cybersecurity, digital inequality and the use of predictive systems in elections. These challenges can affect the integrity of democratic choice itself.51

The crisis, therefore, is not that constitutionalism has become irrelevant. Rather, the constitutional State must learn to recognise new forms of power before they become normalised.52

43. Carpenter v. United States, 585 U.S. 296 (2018).

44. Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar', 24 July 2026.

45. Indian Express, 'Manipur on the boil again: Protests after fresh violence, Internet snapped in valley districts', 11 September 2024.

46. India Today, 'Not going back: Jharkhand aspirants camp in Ranchi over recruitment row', 30 July 2026.

47. Constitution of India, 1950, arts. 14, 19 and 21.

48. Constitution of India, 1950, arts. 14, 19 and 21.

The three Indian case studies also reveal the importance of proportionality. In the Jantar Mantar situation, the constitutional question is not whether public order may be protected; it plainly may. The question is whether AI surveillance and communication restrictions are necessary and narrowly tailored to the identified risk. In Manipur,

public order concerns were similarly invoked to justify Internet restrictions, but the breadth and duration of a shutdown affect the proportionality analysis. In Jharkhand, the focus shifts from surveillance to institutional accountability: citizens demanded a process capable of explaining and correcting alleged failures in recruitment examinations. These examples show that digital constitutionalism must be capable of evaluating both coercive restrictions and technology-mediated administrative decisions.53

CHAPTER 10: TOWARDS A NEW FRAMEWORK OF DIGITAL CONSTITUTIONALISM

A workable framework of digital constitutionalism should begin with the proposition that technological power is subject to constitutional law. The government cannot avoid constitutional review merely because an action is performed through software.54

First, high-risk AI surveillance should require clear legal authority, necessity and proportionality. Intrusive surveillance should ordinarily be subject to independent authorisation, strict retention rules and audit mechanisms.55

Second, significant automated government decisions should be explainable and reviewable. Human oversight must remain available where liberty, employment, welfare or other serious interests are affected.56

Third, large technology platforms should provide transparent rules, reasons for significant content decisions and accessible appeal procedures. Regulation should be proportionate and should respect legitimate private editorial rights.57

Fourth, Internet shutdowns should remain exceptional. Orders should be lawful, narrowly tailored, time-bound and periodically reviewed. Public-order concerns should not automatically justify blanket restrictions on digital communication.58

---

66. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637; Constitution of India, 1950, arts. 14, 19 and 21.

49. M. P. Jain, Indian Constitutional Law (8th edn., LexisNexis 2018).

50. H. W. R. Wade and C. F. Forsyth, Administrative Law (11th edn., Oxford University Press 2014).

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

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

Fifth, an independent institutional mechanism should monitor governmental AI and surveillance practices. Parliamentary committees, courts, data-protection institutions and specialised regulators can together provide oversight.59

Finally, international cooperation is necessary. Global digital rights cannot depend entirely upon the location of a server or corporate headquarters. Minimum international standards should protect privacy, expression, equality and due process.60

Digital constitutionalism should therefore operate as a network of safeguards rather than a single institution.61

An effective framework should also recognise the principle of data minimisation. The fact that information can be collected does not mean that it should be collected. Public authorities should identify the precise purpose for which data is required, collect only what is necessary and establish a definite retention period. Secondary use should require separate legal justification. These safeguards are particularly important for biometric information because biometric identifiers cannot easily be replaced once compromised. Constitutional proportionality should therefore include both the scale of collection and the duration for which information remains available.62

CHAPTER 11: CONCLUSION

The digital transformation has not abolished the classical principles of constitutionalism; it has exposed the need to apply them in new circumstances. Rule of law, dignity, equality, liberty, privacy, freedom of expression, proportionality and judicial review remain the foundation.63

The research supports the hypothesis that classical constitutionalism alone is not institutionally sufficient for the digital age. New forms of technological and private power require additional rules concerning algorithms, data, surveillance and platform governance.64

---

53. Indian Express, 'Manipur on the boil again: Protests after fresh violence, Internet snapped in valley districts', 11 September 2024.

54. Digital Personal Data Protection Act, 2023.

55. Constitution of India, 1950, arts. 14, 19 and 21.

56. Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar', 24 July 2026.

67. Digital Personal Data Protection Act, 2023; Regulation (EU) 2016/679 (General Data Protection Regulation).

57. Constitution of India, 1950, arts. 14, 19 and 21.

58. Indian Express, 'Mobile internet snapped again around Delhi's Jantar Mantar, 6th such order in a week', 23 July 2026.

The Jantar Mantar, Manipur and Jharkhand examples show three dimensions of the problem: surveillance of political participation, restriction of digital communication, and demands for transparency in technology-enabled public administration. They demonstrate that digital rights are increasingly intertwined with traditional constitutional rights.65

The future constitutional order should therefore be technologically aware without becoming technologically dependent. The Constitution should not determine which technology society must use, but it must determine the conditions under which technological power may legitimately be exercised.66

The central principle of digital constitutionalism is consequently simple: technology may change the method of exercising power, but it cannot remove the constitutional duty to justify, limit and review that power. Digital governance must remain accountable to law and ultimately to the dignity and freedom of the individual.67

59. Indian Express, 'Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar', 24 July 2026.

60. Indian Express, 'Manipur on the boil again: Protests after fresh violence, Internet snapped in valley districts', 11 September 2024.

61. India Today, 'Internet suspended in five Manipur districts for 5 days amid student agitation', 10 September 2024.

BIBLIOGRAPHY

Agarwal, Bina, A Field of One's Own: Gender and Land Rights in South Asia (Cambridge University Press 1994).

European Union, Regulation (EU) 2016/679 (General Data Protection Regulation). European Union, Regulation (EU) 2022/2065 (Digital Services Act).
European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act). Jain, M.P., Indian Constitutional Law (8th edn., LexisNexis 2018).
United Nations Internet Governance Forum, official reports and institutional materials. ICANN, official policy and institutional materials on Internet governance.
Internet Society, reports and policy materials on Internet shutdowns and digital rights.

Indian Express, contemporary reports concerning Jantar Mantar, Manipur and Jharkhand protests, 2024–2026.

India Today, contemporary reports concerning Internet restrictions and Jharkhand recruitment protests, 2024–2026.

Constitution of India, 1950.

Digital Personal Data Protection Act, 2023. Information Technology Act, 2000.