

Fundamental Rights in the Digital Era: Reinterpreting Liberty, Privacy and Dignity

Dr. Disha Bangarva*

Assistant Professor, Kanoria School of Law for Women, Jaipur, Rajasthan, India.

*Corresponding Author: dishabangarva@gmail.com

Citation: Bangarva, D. (2026). Fundamental Rights in the Digital Era: Reinterpreting Liberty, Privacy and Dignity. International Journal of Education, Modern Management, Applied Science & Social Science, 08(03(III)), 175–184. [https://doi.org/10.62823/IJEMMASSS/8.3\(III\).9552](https://doi.org/10.62823/IJEMMASSS/8.3(III).9552)

ABSTRACT

The rapid expansion of digital technologies has fundamentally altered the manner in which individuals communicate, access information, participate in public life, conduct economic activities, and exercise personal autonomy. The transition from an analogue to a digitally mediated society has consequently transformed the environment in which fundamental rights operate. In India, constitutional guarantees contained in Part III of the Constitution were originally formulated in an era preceding the internet, social media, artificial intelligence, biometric identification, algorithmic decision-making and large-scale data processing. Nevertheless, the constitutional framework has demonstrated considerable capacity to respond to technological change through judicial interpretation, particularly by expanding the meaning of liberty, privacy and dignity under Article 21 of Constitution of India. The Apex Court of India has played an important role in this constitutional transformation. Land mark judgments such as *Maneka Gandhi v. Union of India*, *Justice K.S. Puttaswamy (Retd.) v. Union of India*, *Shreya Singhal v. Union of India*, *Anuradha Bhasin v. Union of India* and *K.S. Puttaswamy (Aadhaar) v. Union of India* have contributed to the development of a fundamental rights-based understanding of digital governance and technological freedom. At the same time, the emergence of artificial intelligence, facial recognition, pervasive surveillance, data profiling, deepfakes, online harassment, misinformation and platform-based censorship present challenges that cannot always be addressed through traditional interpretations of constitutional rights. This paper examines how fundamental rights and human rights must be understood in the digital era, with particular emphasis on Articles 14, 19 and 21 of the Constitution of India. As these three articles are golden triangle, stated under *Maneka Gandhi v. Union of India* case. It argues that digital constitutionalism requires the protection of not merely physical freedom but also informational autonomy, decisional freedom, digital expression, anonymity, personal identity and human dignity. The paper further examines the relationship between privacy and national security, freedom of speech and online regulation, and technological innovation and constitutional accountability. It concludes that technological advancement must remain compatible with constitutional morality, proportionality, transparency, accountability and the dignity of the individual.

Keywords: Fundamental Rights, Digital Constitutionalism, Privacy, Liberty, Dignity, Article 21, Freedom of Speech, Data Protection, Artificial Intelligence, Surveillance, Digital Rights.

Introduction

The digital revolution that has swept over contemporary society has created a new constitutional landscape whereby technology and fundamental rights come into contact more than ever before. The Internet, smartphones, social media sites, digital money, biometrics, artificial intelligence and cloud computing have become an integral part of daily living. People are communicating, working, studying,

receiving government services, engaging in political dialogue and making purchases using digital technologies. Thus, the enjoyment of many traditional liberties has taken on a decidedly digital character.

The Constitution of India is dated 1950, a time when the technological reality of contemporary society could not even be imagined. However, the drafters of the Constitution intended it to be a living document that can be interpreted according to changing social circumstances. It was drafted in such a way that the language of fundamental rights, especially Articles 14, 19 and 21, allowed the constitutional courts to interpret these rights based on evolving notions of liberty and human dignity.

Perhaps the clearest case would be the evolution of Article 21 itself. At first glance, the right to life and personal liberty might have been a rather narrow concept. However, through the development of Supreme Court's jurisprudence, Article 21 became a repository for various rights which are required for a meaningful existence. For instance, in *Maneka Gandhi v. Union of India*¹, the Court held that all procedures affecting personal liberty should meet standards of fairness and reasonableness.

However, the rise of the digital society has pushed the constitutional discourse even further. It is not only a matter whether one enjoys personal freedom in terms of physical liberty. Now the question is how a person could be autonomous within the reality where one's personal information is constantly collected, processed and commercialized; when one's speech online could be limited either by public or private actors; when one's opportunities and choices are influenced by algorithms; when technologies of surveillance make possible monitoring of people in ways previously unimaginable.

The acknowledgment of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*² marks a constitutional watershed in this regard. Privacy is identified in the nine-judge Bench as a constitutive element of life, personal liberty, dignity, and freedoms under Part III of the Indian Constitution. As per the decision, privacy is not merely the right to privacy but is also the right to bodily integrity, decision-making freedom, informational privacy, and control of one's personal matters.

The advent of digital technologies has therefore brought about a new constitutional vocabulary. Terms such as informational self-determination, data sovereignty, digital identity, algorithmic accountability, technological neutrality, and digital dignity have acquired increasing significance in constitutional discourse.

The focus of this paper is therefore not on whether technology itself is good or bad. Technology could make governance, healthcare, education, economic prospects, and participation in democracy more efficient. What the constitutional question is about is whether technological advancement and its regulation honor individual rights, autonomy, and dignity.

The digital age demands, therefore, that the interpretation of basic rights be revisited rather than discarded. The application of constitutional tenets to new technology should uphold the essence of individual liberty, equality, and dignity.

Objectives of the Study

The main objectives of this paper are:

- To understand the evolving concept of fundamental rights in the light of digital technology.
- To understand the constitutional aspects of liberty, privacy, and dignity in India.
- To understand the judicial evolution of digital rights through Articles 14, 19, and 21.
- To study the contemporary issues concerning surveillance, data processing, artificial intelligence, and online speech.
- To study the issue of balance between individual rights, technological innovations, and government interests.
- To recommend ways for protecting fundamental rights in the context of digital technology.

The approach taken by this paper is doctrinal and qualitative in nature. It is based mainly on secondary sources including the Constitution of India, judgments of the Supreme Court of India, statutory laws, governmental materials, human rights treaties, scholarly articles, and institutional reports.

The constitutional provisions primarily analysed include Articles 14, 19 and 21, in addition to the corresponding provisions regarding equality, free speech and the constitutional remedy.

¹ AIR 1978 SC 597

² (2017) 10 SCC 1

Cases in regard to privacy, personal liberty, internet usage, internet speech, surveillance and data protection are considered for understanding the development of constitutional principles.

This research is purely descriptive and analytical in nature. Primary data collection through interviews and field surveys is not a part of this research. The objective is to analyse the constitutionality of digitalization and formulate a normative framework in this regard.

Fundamental Rights and the Digital Transformation

The concept of fundamental rights has been associated with the role of protecting against abuse of state powers and guaranteeing liberty and equality. Digitalisation brings challenges to the traditional balance between the individual and the state.

In the physical world, identity, movements, communications and transactions of an individual are scattered across space and time. In the digital world, all the above can be compiled into a single data profile. Internet search histories, location data, biometric data, transaction data, social media interaction, photos, and communication can disclose intimate details of the life of an individual.

Therefore, power in the digital environment does not necessarily have to emanate from the usual state machinery only; private technology companies, social media platforms, data intermediaries, and many others may exert influence on individuals.

Here emerges a constitutional problem: should fundamental rights only deal with governmental infringement or does it need to address some form of private technological power as well?

Constitutional law has traditionally concerned itself with the State. But in the digital world, we learn that private companies can make an important impact on the realization of the freedoms of expression, privacy, and access to information. Freedom to speak in public can depend on terms and conditions of use, content moderation systems, and algorithms of distribution.

We need a new conception of constitutional governance for the digital era. The Constitution should defend the individual not only against state oppression, but also against technologies of power that could undermine autonomy, equality, and dignity.

Reinterpreting Liberty in the Digital Era: From Physical Liberty to Digital Liberty

The concept of liberty under the constitution has been significantly altered through judicial interpretation. Article 21 states that no person can be deprived of life or personal liberty unless done through procedure established by law. Through judicial interpretation, this has become a substantive right for numerous other rights.

In the digital age, liberty will increasingly come to mean the ability to make decisions free from undue manipulation or surveillance by technology.

Liberty in the digital age could then mean:

- the right to express oneself online;
- right to information;
- right to digital communication;
- right to digital privacy from arbitrary surveillance;
- right to control one's personal information;
- right to freedom from discrimination through algorithms; and
- decisional liberty in the digital domain.

Liberty will thus have to transcend beyond just physical restraint. Liberty does not necessarily mean physical liberty if the individual's communications are constantly surveilled, decisions are manipulated algorithmically or personal information is exploited without proper consent.

Internet Access and Constitutional Freedom

Internet has emerged as a crucial means through which the exercise of constitutional rights takes place. The fields of education, employment, political communication, journalism, businesses and accessing public services are all dependent on the internet connection.

In *Anuradha Bhasin v. Union of India*¹, the Supreme Court has acknowledged the role played by the internet in exercising the fundamental freedoms. The court has held that the freedom of speech and expression under Article 19(1)(a) and the freedom to practise any profession, trade or business under Article 19(1)(g) are constitutionally protected, and the exercise of these rights through the internet is also constitutionally protected.

What is critical about the judgement is that the Court did not recognise access to internet as an independent fundamental right. The Court only acknowledged that the internet has become an important means through which fundamental rights are exercised.

This makes a difference in a constitutional perspective because while technology may not be a fundamental right per se, it could be the means through which an established fundamental right is exercised.

This brings us to the issue of technological neutrality.

Freedom of Speech and Expression in the Digital Age

Article 19(1)(a) guarantees the right to freedom of speech and expression, which can be regulated by reasonable restrictions under Article 19(2)².

The internet has increased the capacity of the individual to express opinions and disseminate information. Social networking sites have reduced the barriers to political communication, and the individual can engage with audiences without depending solely on the traditional media organizations.

There are also new issues that arise due to digital communication, such as hate speech, threats, harassment, misinformation, impersonation, deepfakes and others.

Therefore, the constitutional challenge is to maintain a proper balance between the right to freedom of expression and regulatory interests.

Section 66A of the Information Technology Act, 2000 was declared invalid in *Shreya Singhal v. Union of India*³ since it violated the right to freedom of speech and expression under Article 19(1)(a).

This decision remains relevant since technological innovations often result in calls for stricter regulations but must be in compliance with constitutional principles.

Novelty is not something that should lead the government to ignore the constitutionality of its actions. Restrictions need to be legal, have legitimate purposes, and be proportionate to those purposes.

Privacy as a Fundamental Right

Recognition of privacy as a constitutional right is the most important event in the development of digital constitutionalism in India.

In the landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁴, the nine judge Constitution Bench of the Supreme Court recognised privacy as a fundamental right under the Constitution. The judgment identified privacy in terms of the rights of life, liberty, dignity, and other freedoms under Part III of the Constitution.

The Court rejected the view that privacy is a narrow elitist right. Rather, it was defined as the basis of individual autonomy and dignity.

Privacy was seen as having the following dimensions:

- physical privacy;
- spatial privacy;
- decision-making autonomy;
- informational privacy; and
- privacy of one's personal identity.

The latter is especially important for the contemporary age of digital technologies. Personal information becomes central for digital platforms. People usually give personal information away in exchange for certain services provided by organizations and corporations without understanding what is being done with their information.

¹ (2020) 3 SCC 637

² The Constitution of India, 1950.

³ (2015) 5 S.C.C. 1

⁴ (2017) 10 SCC 1

It creates an imbalance between an individual and organization. An individual can just click "I agree" on terms and conditions not really knowing what happens to his/her information later. Thus, formal consent does not necessarily guarantee genuine informational autonomy.

An appreciation of privacy in the modern world must include an assessment of:

- What is being collected;
- Why is it being collected;
- How long is it held;
- With whom is it shared;
- If it is used for anything other than its intended use;
- If individuals are able to correct or remove information;
- Automated decision-making based on the collection of such information; and
- Whether there are adequate measures in place against misuse.

Privacy is not simply about secrecy. It is significantly about control, autonomy, and choice.

Digital Dignity

Dignity is at the core of India's constitutional jurisprudence. Dignity forms an essential starting point to consider the interaction between technology and fundamental rights. The concept of dignity requires individuals to be treated as independent beings and not as mere generators of data. Digital technologies can influence individual dignity in many different ways. Publication of intimate content without consent, cyberstalking, online sexual harassment, identity theft, deepfake pornography and constant digital harassment are some ways in which dignity can be severely interfered with.

In the same vein, algorithmic systems have the potential to reduce individuals to mere statistics. When automated processes decide on access to employment, credit, education and public assistance services without appropriate transparency and accountability, the individual becomes an object of automated classification. A dignity-based constitutional framework would require technology systems to honour human agency.

Digital dignity thus entails the right of the individual to:

- govern their personal identity;
- maintain intimate information;
- engage in digital spaces without being humiliated or discriminated against;
- know significant automated processes that affect them;
- contest any erroneous digital classifications; and
- have freedom over personal decision-making.

State Surveillance and Constitutional Limits

Digital technologies have greatly enhanced the power of governments to monitor communications and activities.

Surveillance can be justified for a variety of purposes, such as stopping terrorism, investigating crimes, ensuring national security, and handling public emergencies. Nevertheless, surveillance also involves dangers of arbitrary encroachment upon privacy and liberty.

The constitutional rule is not that surveillance is never to be done. The rule is that surveillance shall take place within the bounds of law and the constitution.

A rights-based approach to surveillance needs to require:

- legal authorization;
- legitimate governmental aim;
- necessity;
- proportionality;
- safeguards of procedure;

- oversight;
- limited storage of information;
- prevention of abuse; and
- a right of remedy.

The rule of proportionality is especially relevant here. In cases where the State acts for a legitimate reason, the method must be rationally related to the reason and cannot impose a disproportionate burden on the rights of individuals.

The threat of uncontrolled surveillance is not only in the risk of direct violation of the individual's rights but in the creation of a society wherein individuals adjust their conduct out of fear of constant monitoring.

Aadhaar Card and Constitutional Privacy

Aadhaar case law highlights the constitutional issues in regard to digital identity systems. The Aadhaar regime intended to put in place a system for creating a biometric identity system used for the authentication of public services. Efficiency, identification, and de-duplication were the key benefits highlighted while constitutional issues included privacy, surveillance, security and possible exclusion.

K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar card judgment) was a case that analyzed the constitutional validity of several aspects of the Aadhaar regime.

In this case, it was clear that digital identity systems have both the capacity to promote public welfare and raise constitutional issues.

The lesson learned from this case is that efficiency alone cannot be a justification for collecting or using personal information.

Artificial Intelligence and Fundamental Rights

Artificial Intelligence is a new phase in the digital revolution as AI machines can process a huge amount of data, find patterns and make decisions or predict outcomes. Their use covers such areas as healthcare, finances, education, law enforcement, employment, administration, and commerce.

- **Transparency Issue**

There is a problem with transparency of many AI algorithms which cannot be easily understood by regular people. If a machine refuses someone a job, services or benefits provided by the state, this person must have the possibility to contest the decision made by the machine.

- **Human Oversight**

Artificial Intelligence cannot take control over human decisions in areas related to basic rights of people. When the automated systems affect the freedom, livelihoods, reputations or access to necessities, there should always be an opportunity for human oversight.

Article 14 and Algorithmic Equality

Article 14 of the Indian Constitution addresses equality before law, but it has now gained increasing significance with regard to digital governance. In traditional equality reasoning, classification and arbitrariness have been the core concerns. However, algorithmic technologies can lead to different forms of indirect discrimination.

An algorithmic decision-making system might employ neutral criteria which have a strong correlation with socially disadvantaged attributes. Thus, in the context of equality in the digital age, the following aspects should be included:

- transparency;
- non-discrimination;
- accountability;
- auditability;
- means of review; and
- reasons for remedy.

Equality principle should stay technologically neutral. Discriminatory result cannot become constitutionally justifiable simply because of the involvement of the algorithm as a tool used instead of the decision maker. Equality is one of the brilliant pillars of Indian democracy.¹

Data Protection and the Individual

With the growing trend of collecting personal data, data protection has become an integral aspect of digital rights.

In India, there have been various changes in legislation in light of these trends, including the enactment of the Digital Personal Data Protection Act, 2023.

It is a step taken towards establishing a regime that deals with the processing of digital personal data and finding a balance between personal interests and the legitimate use of data. But mere legislation cannot offer total protection. In addition to legislation, for proper data governance, the following are required:

- capacity;
- oversight;
- consent;
- security;
- transparency;
- accountability;
- grievance mechanisms; and
- remedies.

Data protection can be viewed in light of the larger constitutional goal of maintaining personal autonomy and dignity.

Social Media, Privacy and the Individual

Social media has collapsed the conventional distinction between private and public aspects of one's existence. People willingly post pictures, thoughts, location, and personal experiences. Nevertheless, the act of willingly revealing something is not equivalent to an individual giving up all privacy rights.

Content posted online can be duplicated, re-published, analyzed, and merged with other data sets. In addition, there are algorithms on social media platforms that decide what content the user is shown. Thus, the question of informational autonomy and manipulation arises. The problem does not lie only in the removal of the content by social media platforms. It is also in the degree of awareness and control users have regarding these algorithms.

• **Deepfakes and Digital Identity**

Artificial intelligence has developed an increasing number of complex synthetic media. Deepfakes can modify images, audio and video to create realistic depictions of individuals who say or do things that never happened. This gives rise to grave consequences for dignity, reputation, privacy and democratic communication.

The issue is especially serious when synthetic material is used for; impersonation; fraud; harassment; non-consensual sexual material; political manipulation; reputational attacks; or misinformation.

Regulation must, however, be careful not to restrict artistic works, satire, scientific research or political discussion. The proper solution will be the one that takes into account context, harm, consent, deception and the rights involved.

• **Right to Privacy versus National Security**

The most challenging question raised by the constitution concerns the relationship between privacy and national security. National security is a legitimate government interest. The State must prevent terrorism, investigate crime and protect the public from danger. On the other hand, the State cannot take advantage of national security to justify any form of unrestricted surveillance. The

¹ M.P. Jain, Indian Constitutional Law, Lexis Nexis, 7th edition.

constitutional concept of proportionality obliges the State to prove a legitimate interest and a rational connection with the means used, as well as ensuring that the interference with rights is proportional.

- **Digitalisation and Digital Exclusion: Equality**

There are various ways of creating inequality through digitalisation.

Persons who do not have access to the Internet, computer skills and smartphones could have problems in accessing services offered by the state, education, job and banking systems. This issue is especially relevant to socio-economically disadvantaged groups, people with disabilities, elderly people and residents of regions which lack adequate infrastructure. Therefore, it is important that digitalisation will not lead to exclusion of those who do not have technological means.

Digital Constitutionalism

This novel idea of digital constitutionalism attempts to extend constitutionalism to the digital world. The basic assumption of this novel concept is that the power generated by technology should be subjected to norms of rights, accountability, and democratic legitimacy. Digital constitutionalism refers to the extension of constitutional values to the new technological realms.

- **The Constitutional Problem of Private Digital Platforms**

The traditional fundamental rights jurisprudence has been mostly concerned with state actions. Yet digital platforms have become powerful enough in both social and economic dimensions. The powerful platforms have the capacity to decide whether the user is able to communicate, publish material, or reach audiences. It is thus an important constitutional issue that a private institution might perform functions which affect public debate, but are not bound constitutionally like state institutions.

Excessive regulation will hamper innovation and private autonomy, while insufficient regulation may let private power to undermine liberty and equality.

- **Privacy and Consent**

Consent has been seen as the cornerstone of data protection. However, for consent to be effective, clicking the accept button alone does not suffice.

If consent is to mean anything, then individuals should have:

- Sufficient information;
- Free choice;
- Simple terms;
- The possibility to revoke consent;
- Alternatives where possible; and
- Protection from coercive data collection practices.

It is impossible for people to have full control in today's digital world. Therefore, privacy cannot be left to the individuals' responsibility. There must also be organizational obligations. Privacy by design, data minimization, purpose limitation and security measures will minimize reliance on individual effort. In the digital age, violation of one leads to a violation of all other freedoms.

Surveillance, for instance, will affect privacy, expression and autonomy. Similarly, misuse of private and intimate data will affect both privacy and dignity and liberty.

The digital revolution of the society cannot be undone, nor should technological advancements be seen as an entity that is antithetical to human rights. The question is how to make sure that the technological innovations grow under the shade of constitutional law. There are a number of ways through which the digital constitutionalism can be promoted in India.

First, the application of fundamental rights in the digital space does not change despite the Constitution being older than all the modern-day digital technologies. The broad provisions of Articles 14, 19 and 21 are a good base to fight with the technological challenges.

Second, privacy is becoming one of the most vital rights in the digital age. The recognition of informational privacy right in Puttaswamy makes a good constitutional ground for data protection.

Third, liberty cannot be perceived only in terms of physical freedom. Digital surveillance, algorithmic manipulation and restrictions to digital expression are capable of affecting the liberty of people.

Fourth, dignity also acquires a new meaning in the digital world. Online harassment, exploitation of private information, identity manipulation and discrimination based on the algorithm are capable of affecting human dignity.

Fifth, technological neutrality is a key constitutional value. There should be no diminishment of rights simply because the exercise of those rights takes place through technology.

Sixth, proportionality must be an element in the balancing of fundamental rights and legitimate government objectives. Both privacy and security should never be considered absolutes in all circumstances.

Seventh, artificial intelligence necessitates a new kind of constitutional accountability. The complexity of algorithms should not be sufficient to prevent them from being subject to constitutional scrutiny.

Finally, digital constitutionalism involves a transition away from seeing people simply as consumers or data subjects, and towards seeing them as constitutional citizens.

Conclusion

The advent of the digital age has changed the context in which fundamental rights can be exercised. Constitutional issues raised by digitalisation thus raise not new questions about the Constitution, but new examples of the timeless principles of constitutional law.

Freedom, privacy and dignity continue to be important to the constitution, but their application will need to change in light of new technology.

Freedom in the digital world goes beyond mere physical freedom. It encompasses the freedom to communicate, access information, take part in digital public life and make autonomous decisions without any technological interference that is not justified.

Privacy does not mean secrecy in the digital world. In a society that constantly collects information on its citizens, privacy means informational autonomy and freedom from being monitored without justification. Likewise, dignity means that one's autonomy and identity must be protected in the digital world too. Individuals should not become mere data points or profiles for technological manipulation.

India's constitutional jurisprudence has already laid the foundation for this evolution. The evolution from *Maneka Gandhi* to *Puttaswamy*, from *Shreya Singhal* to *Anuradha Bhasin* and *Aadhaar* judgment shows how constitutional law can evolve with changing times. Now the challenge will be how these principles are applied in the context of artificial intelligence, biometric technology, predictive analytics, deepfake videos, algorithmic governance, and increasingly powerful digital platforms.

The Constitution must not impede legitimate technological innovation, nor can it let technology escape constitutional accountability. The way forward is a constitutionalism that balances innovation and rights via the principles of legality, proportionality, transparency, accountability and human dignity. Finally, it must be said that the point of digital constitutionalism is not the constitutionalization of technology for its own sake. Rather, it should aim at ensuring that technological developments remain rooted in the human person. The Constitution must continue to play its crucial role of serving as a protective framework against arbitrary powers exercised by traditional institutions and increasingly by data and algorithms.

Thus, the guiding constitutional principle for the digital age might simply be stated as follows: technology can revolutionize the ways in which rights are enjoyed, but it must not undermine the constitutional value of the individual who possesses those rights.

References

1. Constitution of India, 1950.
2. Digital Personal Data Protection Act, 2023.
3. Information Technology Act, 2000.
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
5. United Nations. (1948). *Universal Declaration of Human Rights*.
6. United Nations. (1966). *International Covenant on Civil and Political Rights*.
7. United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*.

Important Judicial Decisions

8. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
9. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
10. *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.
11. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
12. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
13. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
14. *Navej Singh Johar v. Union of India*, (2018) 10 SCC 1.
15. *Joseph Shine v. Union of India*, (2019) 3 SCC 39.
16. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) 3 SCC 1.

Books and Scholarly Sources

17. Austin, G. (1999). *Working a Democratic Constitution: The Indian Experience*. Oxford University Press.
18. Balkin, J. M. (2018). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UC Davis Law Review*, 51, 1149–1210.
19. De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194.
20. Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.
21. Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
22. Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
23. Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

International and Institutional Materials

24. Council of Europe. (2018). *Convention 108+: Convention for the protection of individuals with regard to the processing of personal data*.
25. European Union. (2016). *General Data Protection Regulation*, Regulation (EU) 2016/679.
26. United Nations Human Rights Council. (2012). *The promotion, protection and enjoyment of human rights on the Internet*.
27. United Nations Human Rights Council. (2016). *The promotion, protection and enjoyment of human rights on the Internet*.
28. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO.

