EPH-International Journal of Business & Management Science

A COMPARATIVE STUDY OF SECULARISM, DATA PROTECTION AND SOCIAL CONFLICT IN DIGITAL AGE

Vani Kataria[1*],Dr. Shaharyar Asaf Khan[2] ,Dr. Seema Gupta[3]

[1]Research Scholar, School of Law, Manav Rachna University, Faridabad, India, nehravani@gmail.com , Orcid Id : 0009-0006-2221-4079*
[2]Professor, School of Law, Manav Rachna University, Faridabad, India, shaharyarasafkhan@mru.edu.in, Orcid Id : 0009-0001-8216-0678
[3]Associate Professor, UILS, Chandigarh University, Mohali, Punjab, India, drseemagupta22@gmail.com , Orcid Id : 0000-0001-9289-8759

***Corresponding author:** Vani Kataria

(Email Id : nehravani@gmail.com)

Article History:
Received : 2026-03-02
Revised : 2026-04-11
Accepted : 2026-04-23
Published : 2026-04-30

Abstract:

In this rapidly growing age of technology, democratic and secular nations confront many challenges surrounding digital data, technological algorithms, e-governance, and the evolving online public sphere. This research paper undertakes a comparative study of different models of secularism, like laïcité-French model, principled distance approach-Indian model, separationism-American model, and how these foundational models fit into this new regime of technologies. The paper will further delve into the theoretical lineage of modern privacy law with secular-liberal thought, focusing on Warren-Brandeis ' idea for the concretization of privacy as an individual right. Taking this thought further, this paper will analyze why religious identity is sensitive information that leads to bias and other challenges of discrimination. This research compares the guidelines of different global regimes, like the General Data Protection Regulation (GDPR, 2016), the Digital Personal Data Protection Act 2023 (DPDP Act), and the Digital Service Act (DSA). This paper reveals how each legal system incorporates its secular commitments with evolving technologies. By examining these new developments against growing digital world challenges like AI Surveillance, targeted Profiling, biasness, lack of transparency and accountability, the paper advocates the reassessments of these secular governance models. Looking ahead of time, the research believes that secularism functions as an invisible force, but regulatory systems show us who it is favoring in terms of surveillance, censorship, algorithm bias, and transparency, and there is a need for a comprehensive framework that can harmonize technological advancement with upholding constitutional values.

Keywords: AI, Secularism, DPDP, Bias in Algorithms, Surveillance, Privacy.

Introduction

With the incorporation of AI in almost all disciplines, society has transformed from what it looked like years ago. Similarly, this introduction has also changed the way data is being regulated by the government, how online ecosystems are being managed, and their interaction with citizens. With the introduction of AI in governance, this discipline has also significantly evolved from what it looked like years ago. It has led to the automation of a lot of mundane tasks and has helped people give appropriate words to their thoughts. AI chatbots have also served as a legal tool for laypeople by addressing their legal doubts and issues. Several countries have now started adopting these technologies for speedy resolution of disputes and for improving accountability and efficiency of public institutions, and at the same time, enhancing access to justice.

Building on this, this integration is happening at a time when democratic principles are under threat, public lacks trust in government functioning. In all, this raises doubts on factors like ethical and legal considerations, which also impact society. Among these foundations, secularism, which is traditionally understood as a concept for keeping state and religion in different spheres, plays an increasingly invisible yet decisive role in shaping digital personal data protection regimes. Whether in assessing what constitutes sensitive personal data or setting limitations on state surveillance, or limiting the boundaries of permissible profiling of individuals, a secular perspective gives shape to the architecture of modern data governance.

There is a lack of clarity as to how secularism is linked to technologies and how it is shaping the regulations and formulation of data protection (Müller, 2020). The two terms secularism and technology do not collide with each other, but the perspectives on privacy and secularism can significantly shape the legal mechanism of data protection guidelines and ensure privacy is kept as an important element. In pluralistic societies where religious identity forms a significant axis of vulnerability in digital spaces like sensitive personal data, we need to make these two work together to formulate better guidelines.

The two concepts, digital governance and secularism, together define how societies are shaped, and citizens interact with each other along with the state. On one hand, digital governance helps in including transparency, removing bias, and including governance; on the other hand, secularism in India is followed by principled distance theory, i.e., keeping state and religion separate to promote neutrality in public policy (Linkov et al., 2018; Barocas et al., 2019). When these concepts interact with each other, it promotes transparency, accountability, and access to justice.

Expanding on this, the research article will explore how secularism, digital personal data, and the digital age conflicts interact. It contrasts the models of secularism and analyzes the various modern protection systems such as GDPR, DPDP Act, and many others. The paper will also delve into and discuss the negative effects of the impact of AI on the neutrality of states.

Besides constitutional consequences, modern data protection regulations are increasingly placing high legal burdens upon individual companies, digital platforms, and technology providers that gather, handle, and analyse personal information. Companies working in the virtual world should abide by the rules and regulations established by the government, like the General Data Protection Regulation (gdpr), the Digital Personal Data Protection Act (DPDP Act 2023), and the new AI regulation. These legislations provide compliance obligations with regard to the control of consent, transparency, accountability of algorithms, as well as safeguarding sensitive personal information. In its turn, the meaning of the intersection of secular constitutional principles and digital governance also has a direct effect on the legal compliance of corporations, risk management, and platform accountability of the digital economy.

Theoretical Foundations: Secularism, Privacy, and Digital Data Protection

Rethinking the role of secularism in the digital data protection sphere, examining how modern privacy norms originated from secular philosophies. Although two very different areas,

religion and data, may seem unrelated, the concept of privacy and protection of the same has a strong foundation in secular concepts. This concept of privacy was born with the introduction of 'right to privacy' by Warren and Brandeis in 1890 (Warren & Brandeis, 1890), which was later affirmed by Griswold V. Connecticut ruling. Similarly, many judgements in India affirms the same stance in Gobind V. State of Madhya Pradesh (1975), Kharak singh V. State of Uttar Pradesh (1963) and later Supreme court of India in a landmark judgement of Justice K.S. Puttaswamy (Retd) V. Union of India (2018) case unanimously recognized the constitution recognized the right to privacy as an intrinsic part of the fundamental rights and is covered under Article 21.

DPDP Act 2023 brought a transformation in terms of privacy and data framework in India. This act puts an individual at the center of law, protecting individuals' personal data by embedding principles like informed consent, the right to be forgotten, and minimization of data. On one hand, it gives autonomy to individuals and puts the responsibility on the other hand on data fiduciaries and processors, to keep a check on data protection and other compliance mechanisms (Bekkum & Borgesius, 2022). The Act also created the Data Protection Board of India as a governing central body that will monitor and enforce accountability.

These regulatory frameworks also have compliance obligations to the corporate entities that are considered data fiduciaries or data processors in the view of business law. The use of religious identifiers, which could produce discriminatory results, is prohibited by law, and technology companies, social media, and digital service providers have to introduce measures that will ensure that sensitive personal information is not abused. Non-compliance with such obligations could lead to regulatory fines, reputational risks, and civil liability, and thus, data governance and algorithmic responsibility are an important part of corporate legal compliance. Religious identity of an individual is a sensitive piece of information under various jurisdictions, including the DPDP Act of India, the GDPR of the European Union, and the privacy laws of the US (Bekkum and Borgesius, 2022). This fact shows a secular constitutional safeguarding and adherence to equality and non-discrimination, as well. The reason for employing this is so that this religiously sensitive information is not utilized to treat, exclude, or harm any of the groups unfairly (Petrolini et al., 2022). This categorization of the religious information as sensitive information is a direct development of a secular value that can be outlined in contemporary constitutional democracies (Cabañas et al., 2018).

AI-driven surveillance and profiling systems can trace one's religion by digital trace, biometric data, social media apps, even when that individual wants to keep it private. This can create new problems for minorities, who are being targeted or monitored by states or private entities, undermining the secular Principles guaranteed under the constitution (He, 2024). Despite states' claiming to be neutral and secular, AI systems can lead to bias when the data is limited, or the data feeder is regulated in such a manner that it is against a particular group. This can further lead to algorithm profiling that inappropriately impacts marginalized groups (Ferrer et al., 2021). The research paper also points out that privacy and data protection laws alone are not sufficient to reduce biasness discrimination; there is a more intersectional approach that needs to be developed to equip states to exclude bias and promote equality (Mann & Matzner, 2019). Secularism aspires natural society, but AI Surveillance can reinforce preferences- be it of the state or society. These guises can be in the form of public order, security, and harmony (Sajir, 2023). In some contexts, surveillance is used to determine what constitutes ' legitimate' or 'acceptable' norms (Aizenberg, E & Van Den Hoven, 2020). These actions sometimes lead to social exclusion or discrimination, which undermines the fundamental principles mentioned in constitution of India (Mukherjee, 2025).

Comparative Models of Secularism and Digital Governance Framework

Comparative models of secularism and digital governance can be linked by examining how constitutional principles regulating religion shape the design, content, and institutional logics of digital state infrastructures. Political secularism, either in the form of separationism (as in hard non-establishment) or in the form of principled distance (whereby states engage with

religious communities selectively according to circumstances), establishes a normative standard of what is perceived as neutrality, equality, and non-discrimination in the context of state-building and regulation of digital platforms. Digital governance in the context of separationism would be characterized by apathetic user interfaces, unspecialized users, and homogeneous service norms, and would strive to be as unaware as possible of religious identities in e-government portals, data models, and algorithmic decision-making (Modood and Sealy, 2022). In contrast, in accommodative or principled distance models, online digital systems can also be designed to identify and even distinguish religious communities, such as by supporting multiple religious calendars, or more broadly by offering online grievance and family law services and by formally consulting with religious organizations via participatory online platforms. These variations are overlapping with larger digital governance structures, including both information-centric broadcasting portals, interactive and participatory architectures, since the choice of which data is gathered, how types of identity are coded, and stakeholders are invited to participate in digital policy processes are all mediated by a historically-grounded settlement between religion and political power in any given state. A comparative analytical scheme can thus cross-tabulate forms of secularism and forms of digital governance to anticipate and assess forms of inclusion, bias, contestation, and legitimacy, and note, as an example, how an assertive secular regime might support strong content regulation of online religious expression, whilst pluralist regimes might support strong protection of group representation and accommodation in online public services.

In addition to shaping state digital infrastructures, these governance frameworks also influence the regulatory environment for private technology companies and digital platforms that collect and process large volumes of user data. Businesses operating online increasingly act as intermediaries managing digital identities, algorithmic recommendation systems, and data-driven services. As a result, regulatory regimes such as GDPR and emerging AI governance frameworks impose legal obligations on corporate actors to ensure transparency, accountability, and non-discrimination in automated decision-making systems. Ensuring that corporate algorithmic systems do not reproduce religious or social bias has therefore become a key concern in contemporary digital governance. The differences between Western separationist secularism and the Indian principled distance model can be understood across several legal and institutional dimensions, including the legal stance on religion, state–religion interaction, and focus of protection, as illustrated in Table 1.

Table 1: Comparative Dimensions of Western Separationist and Indian Principled Distance Models of Secularism

Dimension	Western separationist model	Indian principled distance model
Legal stance on religion	Strong non-establishment, minimal state support to religion.	No state religion, but selective support and regulation of multiple religions.
State–religion interaction	Preference for non-interference and arm's- length relations.	Context-specific engagement and reform of religious practices.
Focus of protection	Individual rights of conscience and worship.	Group rights plus individual rights in a multi-religious society.
Role in national identity	Religion is often privatized in official identity narratives.	Religious diversity is integrated into the national identity discourse.

This is how algorithmic systems can undermine neutrality principles, like the US Government's acquisition and usage of Muslim Pro Prayer-app data by USSOCOM, which illustrates a complete breach of state neutrality, as a religious minority digital faith was directly subjected to surveillance (Alrawi, 2024). The research also revealed a significant level of discomfort and a change in behavior among 57% of users, which provoked chilling effects; another feature that highlights the fact that religious freedoms can be suppressed through algorithm profiling (Zuboff, 2019). Lastly, the nervousness of the fact that advanced

predictive analytics are employed to monitor or reason religious behaviour echoes the larger danger of algorithms infiltrating the normal religious existence and making it security-relevant information, and in that way breaching the secular principle of not meddling in any of the religions.

Considering such developments, there exists an increasing necessity of having certain solid legal and ethical standards to protect religious rights in this digital age. The study emphasizes the significance of data transparency in the collection and usage process. Secondly, guidelines on the accountability mechanism should also be made and implemented to keep the government and private organizations responsible for the misuse or discrimination of the data. Third, defining more accommodating frameworks to reflect the religious views of different groups of persons in the digital data policies (Corrêa et al., 2022). These actions are meant not only to ensure the safety of religious freedom but also to ensure that digital surveillance does not develop into a means of religious discrimination or regulation.

The development of key data protection systems in the various jurisdictions shows how the law has eventually recognized changes in digital governance. Key developments are summarized in Table 2.

Table 2: Evolution of Data Protection and Digital Governance Frameworks Across Jurisdictions

Year	Development in laws	Region/Nation
1970-2000	Early privacy/data laws	US, Europe
2016 onwards	GDPR adoption	European Union
2023	DPDP Act	India
2024-2025	Evolving dualism in privacy laws	China

Table 3: Comparative Analysis of Secularism Models and Associated Digital Governance Outcomes

Model	Secularism approach	outcome	Social conflict risk
The US model of strict separation	Strict separation, there is a wall between state and religion	Strong protection of privacy, but no comprehensive national data law.	From low to moderate conflict risk
Laïcité model of France	Strict ban on any religious symbol in the public sphere	Strong neutrality in public space and no comprehensive data collection	From medium to high conflicts, like the Hijab or Niqab controversy
Indian principled distance model	The state engages with religion for reforms.	The DPDP Act allows welfare targeting, but it also creates the risk of profiling.	From medium to high levels of engagement with religious function by the state.
European Union's pluralistic secularism	Diverse secular traditions across different member states.	GDPR classifies religion as a special category of data. The EU has strong AI and platform regulations (AI Act, DSA)	Low to strong anti-discrimination and full digital governance.

Different secularism models influence digital governance approaches and may produce varying levels of social conflict risk when implemented within technological infrastructures. A comparative overview is presented in Table 3.

Sensitive Personal Data and Secular Constitutionalism

There are many legal frameworks that show that the right to privacy, the right to information, and the right to the protection of personal data are a deeper commitment of constitutional secularism and the new privacy laws like DPDP Act, GDPR, and U.S Civil rights-based privacy rules. The definition of religious data as "sensitive personal data" needs to be protected as the need for equal treatment, state neutrality, and laws against discrimination are base of constitutional and privacy laws (Quinn, 2020). In many frameworks, religion is specified to be the highest level of protection, as there has been a long history of misuse of the same by all nations. Secular constitutionalism recognises religious affiliation as a risk that carries many stigmas like targeted monitoring, bias, intrusion by state agencies, especially in multilayered, multidimensional, and multireligious societies (Gstrein & Beaulieu, 2022). By conceptualizing these religious data in these technologies, these nations aim to prevent overt discriminatory practices as well as subtle algorithmic harms that might replicate historical prejudice or generate new forms of profiling in this AI world.

The basic structure doctrine, devised by the SC of India, constitutes a part of the basic structure of our constitution and thus requires even stronger safeguards to ensure that no community is affected due to underlying religious identity (Kesavananda Bharati v. State of Kerala, 1973). This religious identity is often accompanied by factors, such as class, caste, language, and religion, often leading to compounded vulnerabilities that can further be exacerbated by intrusive surveillance or unchecked data processing. In data protection laws like DPDP for India, it is broader in sense than GDPR, special preferences are to be given to rights like equality, equal treatment to all citizens, no discrimination on bases od caste, religion, etc., and giving its due to privacy, i.e., Article 14, 15, and 21. This will result in a digital system foundation that will prevent social inequalities, which is also a constitutional responsibility of any law formulated in the nation. When analysis of data is done by identification of names, addresses, activities on online platforms of the comments, likes, etc., and other similar markers, by using AI, it creates a mapping for disclosed or inferred religious data, which leads to making these constitutional safeguards all the more important than ever. Based on this discussion, it can be concluded that religion can be termed as sensitive data, but as our constitution entails, secularism needs to be upheld, and new technologies should align with these standards of norms and ethics (Mann et al., 2018).

AI Surveillance, Algorithmic Profiling and the Crisis of Secular Neutrality

Artificial intelligence, an increasingly used tool for searches, sorting, and analysing data, has the potential to exacerbate surveillance and profiling for both government and private players. This has become one of the challenges for secular constitutionalism as the state has to protect an individual against any biasness either from humans or AI-based (Papakostas, 2025). In the digital era, algorithms are more and more capable of making religious identity assumptions based on indirect clues, e.g., names, eating habits, the use of prayer apps, moving around during festivals, and social-network affiliations. These conclusions are frequently made without permission, and any state or private platform may build an invisible religious profile, which consequently may influence policing, welfare targeting, or platform modulation. The examples of the U.S. military buying Muslim Pro data, the historical misclassification of ethnic minorities by facial recognition predictors, and the Aadhaar-based welfare discrimination reveal that even the most neutral technologies may have an unequal influence on certain religious groups. These practices corrupt secular neutrality through engraining the already existing social bias into automated decision-making systems and, as a result, making surveillance appear objective but reproducing discriminative patterns (Afroogh et al., 2024).

On top of state surveillance, privately employed technology firms that write and implement artificial intelligence systems are also under growing legal pressure. When algorithmic models are used to achieve specific advertising, predictive analytics, content moderation, or recommendation services, businesses that use these algorithms may create discriminatory results unintentionally in situations where biased data sets are used or where the decision-making process is not transparent. As a result, the regulatory discussions in places like the

European Union are increasingly focusing on corporate responsibility and transparency in algorithms and compulsory impact analysis of high-risk AI systems used by companies and online services.

India, in its constitution, has placed secularism as part of the basic structure of the constitution. The theory of "basic structure" contemplates that there are certain features of the constitution which form its core and cannot be amended so as to become redundant. These principles represent the soul of the constitution (S. R. Bommai v. Union of India, 1994). The introduction of AI-based technologies with coding embedded with pre-existing social biases into automated decision-making technologies raises fundamental questions with respect to principles such as Equality ("Article 14"), Principle of Non-Discrimination ("Article 15"), and right to privacy and dignity ("Article 21"). AI-enabled technologies, which have an opaque decision-making process or which are manufactured without any fairness safeguards, have the potential to disproportionately affect minority groups by subjecting them to greater scrutiny, predictive policing, moderation of content, or digital exclusion (Constitution of India, 1950a; 1950b, 1950c). This problem is further heightened by the "black box" decision-making process of AI-based technologies, which makes it harder to determine the reasons behind a particular decision taken by these technologies and makes it difficult for individuals impacted by such decisions to understand, contest, or challenge religiously skewed decisions (Mann & Matzner, 2019). This leads to a slow yet "unnoticed erosion" of the basic principles of the Constitution. Secularism is meant to play a balancing function in society through fir segregation of the government and religion, which is further disrupted by AI through amplification of hate speech, accelerating communal polarization in society, and influencing online visibility or excessively censoring a particular community online. This integration of AI surveillance and profiling of people on religious grounds signals an incoming crisis of secular neutrality, where the communities are being watched, flagged, or marginalized based on technological infrastructure prevalent rather than on the basis of state policies defined in that respect. Thus, this poses a grave threat to the promise of secularism enumerated in the Constitution.

Conclusion

The paper concludes that the DPDP Act'2023 is a landmark in the course of protecting privacy and requiring a secular digital ecosystem. Paper makes sure that true neutrality must be not only slightly fixed with technical tools but also a strong legal, ethical, and social protection of secularism, and encourages equality in the era of AI. The AI systems are not technologically neutral and instead actively replicate and strengthen the existing social hierarchies in terms of caste, gender, class, and religion because they are designed based on biased data and opaque design decisions. It brings about a grave constitutional issue in India, though Articles 14, 15, and 21 stipulate equality, non-discrimination, and informational privacy; modern frameworks such as the DPDP Act, 2023, do not focus on algorithmic bias, impose fairness, explainability, or human control. The experience of the EU AI Act, US algorithmic accountability controversies, and the control-based model of China demonstrate that rights-based, risk-based regulation, mandatory impact evaluations, and rigorous enforcement are currently becoming new international standards. In the case of India, the article suggests that it is not possible to protect the data, but an extensive AI law, an autonomous AI control agency, mandatory bias assessment, and Algorithmic Impact Assessment of the risky systems (welfare, policing, hiring, credit) should be performed, human-in-the-loop defense, and transparent algorithms in government affairs are required. Finally, the legal responsibility of AI is a constitutional requirement and privacy, autonomy, and equality should be maintained. If left unregulated, algorithmic governance will quietly erode secular–democratic commitments to equality, dignity, and non-discrimination, especially for already marginalized groups, so in order to safeguard it, we need to reevaluate both AI and societal structures and uphold all fundamental principles. Regarding business law, the given developments highlight the increasing importance of corporate regulatory compliance in online spaces. The companies that manipulate personal data have to enact

governance concerns, including algorithmic audits, data protection impact assessment, as well as AI compliance frameworks that would guarantee transparency, accountability, and legal compliance.

References

1. Müller, T. (2020). Secularisation theory and its discontents: Recapturing decolonial and gendered narratives. Debate on Jörg Stolz's article on secularization theories in the 21st century: Ideas, evidence, and problems. Social Compass, 67(3), 315–322. https://doi.org/10.1177/0037768620917328
2. Linkov, I., Trump, B., Poinsatte-Jones, K., & Florin, M. (2018). Governance strategies for a sustainable digital world. Sustainability, 10(2), 440. https://doi.org/10.3390/su10020440
3. Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning: Limitations and opportunities. MIT Press.
4. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.
5. International Journal of Law, Communication & Work. (n.d.). Retrieved from https://ijlcw.emnuvens.com.br/revista/article/view/84
6. Bekkum, M., & Borgesius, F. Z. (2022). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? Computer Law & Security Review, 48, 105770. https://doi.org/10.1016/j.clsr.2022.105770
7. Petrolini, M., Cagnoni, S., & Mordonini, M. (2022). Automatic detection of sensitive data using transformer-based classifiers. Future Internet, 14(8), 228. https://doi.org/10.3390/fi14080228
8. Cabañas, J., Cuevas, Á., & Rumín, R. (2018). Unveiling and quantifying Facebook exploitation of sensitive personal data for advertising purposes. Proceedings of the 2018 World Wide Web Conference, 479–495.
9. He, Y. (2024). Artificial intelligence and socioeconomic forces: Transforming the landscape of religion. Humanities and Social Sciences Communications, 11, 1–10. https://doi.org/10.1057/s41599-024-03137-8
10. Ferrer, X., Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: A cross-disciplinary perspective. IEEE Technology and Society Magazine, 40(2), 72–80. https://doi.org/10.1109/MTS.2021.3056293
11. Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society, 6(2). https://doi.org/10.1177/2053951719895805
12. Sajir, Z. (2023). A post-secular approach to managing diversity in liberal democracies: Exploring the interplay of human rights, religious identity, and inclusive governance in Western societies. Religions, 14(10). https://doi.org/10.3390/rel14101325
13. Aizenberg, E., & Van Den Hoven, J. (2020). Designing for human rights in AI. Big Data & Society, 7(2). https://doi.org/10.1177/2053951720949566
14. Mukherjee, S. (2025). Algorithmic bias and discrimination: Legal accountability of AI systems. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences. https://doi.org/10.37082/ijirmps.v13.i4.232659
15. Modood, T., & Sealy, T. (2022). Developing a framework for a global comparative analysis of the governance of religious diversity. Religion, State & Society, 50(4), 362–377. https://doi.org/10.1080/09637494.2022.2117526
16. Alrawi, A. (2024). Algorithmic profiling and the threat to religious expression: The case of Muslim Pro. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4901654
17. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
18. Corrêa, N., Galvão, C., Santos, J., Pino, C., Pinto, E., Barbosa, C., Massmann, D., Mambrini, R., Galvao, L., & Terem, E. (2023). Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. Patterns, 4, 100857. https://doi.org/10.1016/j.patter.2023.100857

19. Quinn, P. (2020). The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. German Law Journal, 22(8), 1583–1612. https://doi.org/10.1017/glj.2021.79
20. Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35. https://doi.org/10.1007/s13347-022-00497-4
21. Kesavananda Bharati v. State of Kerala, (1973) 4 SCC 225. Retrived from: https://indiankanoon.org/doc/257876/
22. Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia. International Communication Gazette, 80(4), 369–384. https://doi.org/10.1177/1748048518757141
23. Papakostas, C. (2025). Artificial intelligence in religious education: Ethical, pedagogical, and theological perspectives. Religions, 16(5). https://doi.org/10.3390/rel16050563
24. Afroogh, S., Akbari, A., Malone, E., Kargar, M., & Alambeigi, H. (2024). Trust in AI: Progress, challenges, and future directions. Humanities and Social Sciences Communications, 11. https://doi.org/10.1057/s41599-024-04044-8
25. S. R. Bommai v. Union of India, (1994) 3 SCC 1. https://indiankanoon.org/doc/60799/
26. Constitution of India. (1950). Article 14: Equality before law. Government of India.
27. Constitution of India. (1950). Article 15: Prohibition of discrimination on grounds of religion, race, caste, sex, or place of birth. Government of India.
28. Constitution of India. (1950). Article 21: Protection of life and personal liberty. Government of India.
29. Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society, 6(2). https://doi.org/10.1177/2053951719895805