LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Data Protection in the Era of Artificial Intelligence: Legal challenges of Automated Decision-Making and Digital Surveillance

Author
Gaurav Bijarnia

Data Protection in the Era of Artificial Intelligence: Legal challenges of Automated Decision-Making and Digital Surveillance

Gaurav Bijarnia
BBALLB(H), Semester -10
Amity University, Noida, Uttar Pradesh
Enrollment Number – A3221521180

Abstract
With digital technologies spreading like wildfire in our lives, and endless rivers of data rushing around us and computers taking more decisions every day, the meaning of privacy and control over information has become very fluid. As information becomes ever more valuable, the question of who can do what with it is becoming a concern for legislators, policy experts and designers. This study of contemporary issues surrounding protection of data will shed light on global surveillance, fact-finding from millions, cross-border data flows, and the sophisticated calculations behind online services. We will also look at the historical significance of privacy, starting in the use of protecting one's reputation and secret, and expanding this notion to include having control over how information is used in the digital realm.
This paper will compare the current legal regimes to examine whether it helps protect citizens against exploitative data practices of governments and corporations. I will use the example of the EU's GDPR, the Data Protection Act in the UK, and the new digital personal data law that India is implementing in 2023 to observe how individuals are actually protected and how they can be consulted. Comparing the current laws will show similarities, both in terms of the goals, and areas in which these efforts fall short. There is no easy comparison between countries with similar legal regimes, as different countries may have different approaches to handling data protection, which will be enacted on their own priorities.
Technology catches up with laws. With artificial intelligence, tracking users, body identifiers, predictive algorithms, or mass surveillance, small gaps in software decisions can quickly become large ones; cybersecurity risks can increase; automatic systems make decisions without being told; and the transfer of personal data across borders goes through opaque channels and could jeopardize people's freedoms, transparency, and accountability. Sometimes, it is the dilemma between a privacy and state security concern, policing and law enforcement needs, public health, and business development that must be addressed; the research will address these dilemmas and attempt to identify ways to improve the right, consent, the best

use of data collection, minimizing data collection, and continue progress in invention.

This research takes advantage of a variety of methods, both deep analysis of a law's jurisdiction and comparing them against one another to identify where rights to privacy have been protected from widespread technology surveillance and abuse of data. It does not just give a brief history of the law, but also recent court decisions, legal literature, and the most recent research, and attempts to explain how the online realm is being protected. Lessons from the field of encryption, data anonymization, and privacy-preserving systems are incorporated into the study, and checking whether the law guarantees comprehensive protections individual rights is offered through its legal system is essential. In many cases, gaps are clearly apparent, suggesting that the law is beyond its age and should be addressed.

Evolution of Data Protection as a Fundamental Right

Historical Development of Privacy Rights-

Over time the concept of privacy has evolved tremendously. It has changed from the rather limited protection of physical space to encompassing rights of autonomy, dignity and control over one's information. In the early days of the law, it was not treated as a separate right, but was rather protected by existing law, such as property law, laws against trespass and rules concerning confidential information. Society and technology have developed, particularly with the rise of electronic communications and mass media, making a specific right to privacy a more concrete need. The concern for privacy emerged in the 1800s as a result of technologies such as photography and sensationalist reporting, giving rise to the recognition of a right to privacy, distinct from a right to property. Privacy as an interest grew into something larger which encapsulates all of the various rights which people feel they have against undue intrusions into their personal lives, their communication and their data. Today privacy is becoming more and more intertwined with data protection particularly when looking at the areas of AI and electronic surveillance.[1]

Warren & Brandeis: The Right to Privacy-

The Harvard Law Review featured "The Right to Privacy," an important article by Samuel D. Warren and Louis D. Brandeis, that was published in 1890. This article is a pivotal document in the history of the law of privacy and it is a widely held belief that it serves as the foundation of modern privacy law. Warren and Brandeis called for recognition of a distinct right of privacy-which they called - the right to be let alone. They emphasized the need for people to be safe from physical intrusion and from unauthorized dissemination of their private information. The argument was that

[1] **Griswold v. Connecticut**, 381 U.S. 479 (1965)

existing legal remedies, such as defamation and property law, were inadequate to deal with new forms of intrusion enabled by technology.
The article described the historical context of the development of privacy torts in the common law: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of likeness.
It also had an effect on constitutional and human rights law, changing the way people think about privacy as an important part of their freedom and dignity.[2]

Article 12 of the Universal Declaration of Human Rights (UDHR) establishes one of the earliest and most influential formulations of the right to privacy in international human rights lawWhich states that "No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his honor and reputation" and that "everyone has the right to the protection of the law against such interference". It is significant that the article views privacy as very wide, and it includes personal life, home and correspondence in its definition of privacy as well as protection against physical trespass. The word "arbitrary" means that even legal interference must meet standards of reasonableness, necessity, and proportionality. This is the basis for modern privacy law. Article 12 also makes a strong connection between privacy and human dignity by linking privacy to honor and reputation.
In spite of its lack of legally binding force, the UDHR and Article 12 in particular, has demonstrated a powerful normative effect, influencing the development of constitutional provisions and privacy legislation worldwide, as well as acting as an influential model for future binding treaties.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR)
The right to privacy a legal duty for State Parties. It says again that no one should have their privacy, family, home, or correspondence interfered with in an arbitrary or illegal way, and it promises legal protection against such actions. The words "arbitrary" and "unlawful" create a double standard. This means that in a democratic society, interference must not only be allowed by law, but it must also be fair and reasonable. This increases privacy protections in a fundamental way, by prohibiting the abuse of state power. Furthermore, Article 17 sets out positive as well as negative duties on states. The duty not to interfere without reason, and also the duty to create laws and machinery for the protection of citizens against such interference by private as well as public actors. The Human Rights Committee of the United Nations expanded on the understanding of Article 17 by stated that Article 17 extended to all new dimensions of privacy, including the need for personal data protection, and

[2] **Roe v. Wade**, 410 U.S. 113 (1973)

limitations on surveillance through new forms of technology. Particularly relevant for our modern age of artificial intelligence and big data, Article 17 is a key framework within which the legality of surveillance and automated data processing can be assessed. In sum, Article 12 UDHR and Article 17 ICCPR represent the backbone of international privacy law and enshrine principles of dignity, autonomy, and legal protections, that form the basis of contemporary data protection legislation.

1.Informational Self-Determination –

Informational self-determination-the cornerstone concept of modern data protection law, referring to the individuals' rights to know, control and influence the processing of their personal data-stems from the general notions of privacy, dignity, personal autonomy. It evolved beyond traditional notions of privacy in the age of the Internet, emphasizing on data management and individuals' participation in the "information society", where personal data becomes deeply interwoven with individuals' identities and freedom. Such rights were developed and imposed because increasing amount of personal information were stored on computers and integrated processing was dangerous. Informational self-determination ensures individuals do not turn into subjects who are simply being collected and handled, and has four components: informed consent right, knowledge right, data correction and access right, and restriction of processing and objection right. It also means that both the government and private companies can't collect too much or unnecessary data. Informational self-determination becomes even more important when it comes to artificial intelligence. AI systems need a lot of data, which often includes private information about people. People risk losing control over their digital identities if there aren't good ways to keep them in check. The idea also talks about things like profiling, automated decision-making, and predicting behavior, which can affect people's choices and freedoms.

1. **German Census Case (1983) –**

The concept of informational self-determination, while having earlier underpinnings, was established in the landmark German Census Case of the German Federal Constitutional Court. The German Census Case involved several citizens who challenged a census law passed by the German government that demanded extensive personal information from citizens covering various aspects of their lives including their private lives and social circumstances. The constitutional challenge was brought forth by several citizens. In this landmark decision the Court concluded that unlimited collection and processing of personal information threatened the liberty of the citizen and the nature of democracy. The Court developed the concept of informational self-determination as a constitutional right which draws from the fundamental right to human dignity and the general personality right under the

German Basic Law. In essence, the individuals have control over their personal information. It is important to control the context in which, when and by whom their information may be accessed and processed.

The Court raised one of the most significant concerns in this decision and it relates to the idea of a 'transparent citizen,' and the danger of constant monitoring and profiling as individuals' lives could become fully discernible through the information gathered on them. The Court warned that this potential monitoring could induce self-censorship because individuals may change their behavior out of fear that they might be watched, creating a 'chilling effect' inconsistent with democracy and freedom. This led to the invalidation of parts of the law and to the imposition of strict requirements for the collection of personal information: need for clear and transparent rules and legality, proportionality, and purpose limitation.
The German Census Case was a breakthrough in the area of data protection and was the basis for many modern-day frameworks such as the European data protection principles and the GDPR.[3]

2. Control over Personal Data –

Control over personal data is an essential aspect of informational self-determination. Control refers to the right of an individual to oversee the collection, use and disclosure of personal data relating to themselves. This can be facilitated through various legal and procedural mechanisms which serve to prevent unreasonable and/or arbitrary processing of personal data by individuals.

One such tool is informed consent. Herein, individuals need to be informed about all uses of their personal data before their data is collected and there has to be informed consent. Consent must be given freely, it is defined as 'unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies his or her agreement to the processing of personal data relating to him or her.' Consent mechanisms have, in reality been accused of failing and being impotent due to an imbalance of information and lengthy, opaque privacy policies and the user is unable to retain control of their data if they do not understand how it is being used.
The principle of purpose limitation is another key principle. It means that personal data should be collected for stated, legitimate purposes and not further processed in a manner incompatible with those purposes unless the data subject consents to that further processing. The principle attempts to limit "function creep," the practice of

[3] **Digital Rights Ireland Ltd v Minister for Communications**, Joined Cases C-293/12 & C-594/12
Struck down EU Data Retention Directive; emphasized data protection as a fundamental right separate from privacy.

using data collected for one purpose for another, totally different purpose. This relates to the principle of data minimization which complements purpose limitation in that only that data necessary to fulfill the purpose it was collected for, will be gathered, thereby minimizing data at its roots.

A crucial aspect of control over personal data include data subject rights: individuals possess the right to access personal data relating to them, the right to have incorrect personal data corrected, the right to request erasure of personal data relating to them (the right to be forgotten), and the right to restrict or object to processing of personal data relating to themselves.
These principles of controlling personal data can be found in modern legislation like General Data Protection Regulation (GDPR), and the Digital Personal Data Protection Act, 2023. While on the one hand modern instruments ensure protection of privacy, they do not appear to keep pace with advancing technologies like big data and artificial intelligence. With increasing automation of data collection, profiling, and extensive cross border data flows, an individual is increasingly unable to effectively exercise control over personal data.

Data Protection as an Independent Right-
Data protection used to be considered merely an extension of privacy. As a result of the development of new technologies, the enormous amount of personal data collected and the development of artificial intelligence, data protection has gradually acquired an autonomous status as a legal right, which is distinct from privacy and has its own legal regime, principles, and extent. The scope of data protection is different from traditional privacy, because while traditional privacy is mainly used to prevent the intrusion into private life and space of individuals, the right to data protection is applied to the systemic processing of personal data, irrespective of whether the latter is intrusive. The notion that data protection should be an autonomous right also originates from a change in our understanding of personal information in the digital era. Indeed, as opposed to former times when personal information was passively collected and only at individual's will, personal data is now constantly and actively collected, stored, processed, and disseminated by both the state and other entities and constitutes a source of risks like surveillance, identity theft and misuse, particularly due to the possibilities for systematic profiling and tracking that it has created. Specific provisions have thus been enacted to provide a new regime regulating data processing. The principles governing data protection as a right include lawfulness, fairness and transparency, limitation of purpose, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability. These rights apply to each and every kind of data processing, even when there is no intrusion into the personal space of an individual. Data protection

may thus have more extensive effects.[4]

Article 8 of the EU Charter –

1. Article 8 of the Charter of Fundamental Rights of the European Union makes it very clear that data protection is a basic right. This clause says:
   a. "Everyone has the right to have their personal data protected."
   b. "Such data must be processed fairly for certain purposes and with the consent of the person concerned or some other legal basis set out by law." Everyone has the right to see the information that has been collected about them and to have it corrected.

2. The rules of this protocol shall be monitored by an independent body."

The fact that Article 8 clearly distinguishes data protection from the right of privacy, a right guaranteed by Article 7 of the same Charter (which guarantees a right to private and family life), marks this article as particularly important. In addition to privacy, an explicit right relating solely to personal data is now enshrined in the charter.

The Article introduces the following key aspects:

An autonomous right: Data protection as a separate right rather than merely a component of the right of privacy;
Lawful and fair processing: Processing that is transparent and in accordance with relevant legislation;
Purpose limitation: data must be processed for specified and lawful purposes;
Consent or other legal basis: that processing of data must either have the consent of the person to whom the data pertains or be covered by some other legal basis;
Access and rectification: data subject rights to access and amend their personal data;
Independent supervision: that monitoring of such rules must be by an independent body.

Article 8 is responsible for the progression of European data protection and has played an integral role in the evolution of the GDPR and consequently other global data protection rules.[5]

Separation from Traditional Privacy –

The demarcation between data protection and privacy is an essential legal development of the contemporary jurisprudence. Although both these rights bear a

[4] **Google Spain SL v AEPD**, Case C-131/12
Recognized the "right to be forgotten," reinforcing individual control over personal data.
[5] **Schrems v Data Protection Commissioner**, Case C-362/14

high degree of correlation and intersect each other, the two can clearly be differentiated in the degree, nature of the goal they serve and method of regulation.
Privacy in its traditional sense deals with shielding of an individual's life from unnecessary intrusion into his personal and private space, say spying or unwanted visits to one's home or an invasion of intimate details of the personal life of a person, etc. Its principal concern is to maintain personal dignity, integrity and a safe personal space and any breach of privacy is direct invasion of an individual's private life.

Data protection is concerned with the handling of personal data, which may or may not constitute invasion of privacy in its traditional sense and involves a regulation of collection, storage, use and sharing of personal data in the normal course of affairs. A company maintaining customer data will not be violating an individual's privacy in its traditional sense while holding such data, but will definitely have to adhere to the law on data protection.

One other significant differentiating factor is the means of protection. Traditionally, privacy is defended through constitution or tort and violations are dealt with post them. Data protection is however, governed by specific legislations laying down mandatory obligations on the controllers and processors of data, such as compliance mechanisms, audit and penal provisions.
Further, the concept of data protection lays much emphasis on the procedural aspects and rights such as the right of access, correction, deletion and restriction of processing of personal data and includes elements such as accountability and data governance that are traditionally not the concern of privacy.
Division of these rights from each other arises from the exigencies of the new digital era. If privacy shields a person's private space, data protection ensures that a person continues to hold sway over his information in an environment of constant stream of data.[6]

Indian Perspective:

1.Article 21 and Expansion of Personal Liberty –

There is no express mention of right to privacy in Indian Constitution but this right has been impliedly read by Indian Judiciary into Article 21 of Indian Constitution which states 'No person shall be deprived of his life or personal liberty except according to procedure established by law". Gradually this article has been interpreted so widely that it is considered not only a procedural safeguard but also a broad guarantee of rights. Early cases like A. K. Gopalan V. State of Madras (1950)

[6] **European Data Protection Board**,

adopted very restrictive interpretation of personal liberty but this view of judiciary has been shifted to an ever-increasing liberal view following case Maneka Gandhi V. Union of India (1978) where the courts stated that 'procedure established by law' must be just, fair and reasonable. From this stage onwards this article has been stretched to cover all human rights needed to lead a life with dignity such as right to life and liberty, health, education, livelihood and clean environment. It was under such interpretation that privacy was deemed to be an aspect of personal liberty, since no right would be of any significance to a human if he did not enjoy control over his personal life.[7]

2. K.S. Puttaswamy v. Union of India (2017) –

One ruling is different, buried deep in India's legal history. Not because it screamed change, but because it quietly affirmed what many sensed as true all along. Where silence was golden, nine voices spoke as one in a courtroom. Privacy — the thing so much talked about, so much questioned — was finally recognized as the natural birthright of every man. This did not happen by protest or policy but by careful reading of existing promises. The decision was deeply rooted in Article 21 and thus dignity was woven into protection. The Constitution itself did not change; only its words became clearer.

One person's challenge to India's Aadhaar program ignited a larger debate about data gathering — especially fingerprints and other personal details collected.

Did the Constitution indeed protect privacy? This turned into the essential question. The court confirmed this, and put aside earlier decisions that had previously hindered such a concept. Earlier judgments like M.P Sharma versus Satish Chandra (1954) and Kharak Singh's decision (1962) were overruled since they opposed the emerging understanding of privacy. Privacy could now triumph - not overriden by outmoded understandings.

The peculiar feature of this verdict is that it recognizes privacy not as a singular entity, but as a layered concept like body, data, and choice. Dignity is tightly interwoven with each of these layers by virtue of being who we are. Autonomy in this regard is what has immense significance. Any limitation should now have an established basis. While this could be law, the ruling also suggests the requirement for the state to demonstrate genuine need and balance. The value of what is given up compared to what is acquired should be evaluated carefully.

Online, with the compilation of fragments of personality as a consequence of every click, there is little that can be more vulnerable. In one ruling, the court notes that, 'Bits of identity tend to slip out of control when computers are employed to observe human behaviour in an unchecked manner,' and in this fast- paced age, "rules and

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

mechanisms cannot keep up with the speed of technologically driven developments," (2009) and as such greater vigilance and security measures need to be taken since damage may not be identified as and when it occurs.

3.Privacy as Intrinsic to Dignity and Autonomy –

The notion of dignity and autonomy has played a significant role in shaping the Indian jurisprudence on privacy. In particular, the Supreme Court judgment in Puttaswamy declared that privacy is more than just a negative right-freedom from invasion-but a positive right to formulate one's own choices.

This positive conception of privacy protects one's right to privacy relating to deeply personal choices-such as regarding marriage, family, sexuality, Procreation and lifestyle-and, informational privacy-the right to control over one's personal data which is an aspect that is particularly relevant in the domain of Artificial intelligence and technologies based on data, that employ data for extensive profiling and decision-making purposes.

In this regard, autonomy relates to the capacity to direct and make informed decisions regarding one's own life, a capacity for which privacy is an essential prerequisite. This may relate to what and what not to disclose of their personal information or the beliefs they should hold or how to lead their life and privacy protects the individual from undue interference in such decisions.

Modern technologies like Artificial Intelligence and data-driven systems make the concept of dignity and autonomy as integral components of the privacy right ever so relevant. Automated decision-making and large-scale surveillance can significantly limit an individual's choices and also cause a "chilling effect"-where one is forced to change one's own conduct out of apprehension of being monitored. Viewing privacy as intrinsic to autonomy and dignity, the constitutional position under which such technologies are evaluated remains unshakeable.[8]

Relevance in Digital and AI-Driven Societies-

These days, keeping personal info safe matters more than ever because tech and artificial intelligence are everywhere. Digital spaces shape much of daily living now - people leave traces constantly, just by using apps, posting online, paying bills, visiting doctors, or running gadgets at home. Because so much detail gets collected, private data has become powerful stuff. Guarding it well means protecting who we are, what we do, how we live.

Most people do not realize how much detail gets gathered when AI tools work behind the scenes. Because these systems need massive amounts of information to

[8] **A.K. Gopalan v. State of Madras**, AIR 1950 SC 27

operate, they track actions constantly - sometimes without clear notice. Hidden patterns emerge through repeated observation, which quietly pulls private moments into digital view. Control slips away before many even know there was something to lose. Yet choice still matters; deciding who accesses your details remains a basic right, not a privilege handed down.

One big concern involves machines making choices that affect people's lives - jobs, loans, medical care, policing. Even though automation speeds things up and keeps results uniform, it brings up questions about who answers for mistakes. When hidden code decides outcomes, appealing those choices gets tough, particularly if users do not know what happens behind the scenes. That reality pushes demand for laws requiring clear reasoning and real-person supervision built into artificial intelligence tools.

Watching people online makes clear how much privacy matters when machines shape daily life. Governments along with companies now rely more on tools like face scans, body data tracking, eye movement analysis to keep tabs on citizens. So if safety or paper-work is the explanation or justification used when these technologies are introduced, the overuse is a continuous erosion of fundamental rights. Endless surveillance creates an "unobtrusive regime... Which slowly erodes freedom of speech and individual autonomy by inducing a constant feeling of being watched."

What truly distinguishes the Puttaswamy judgment? It grounds the right to privacy in a constitutional framework and centers on dignity and autonomy. Dignity and autonomy become fundamental at a time when fragments of our lives are endlessly streaming on digital networks. If any right has to have limits it has to be guided and there should be a series of tests to determine what limitations on this right may be introduced: are there laws, are the intrusions necessary and is it proportionate? The tests here are also instructive for the development and implementation of AI in a legal framework:

Provisions like the General Data Protection Regulation (GDPR) and the Indian Digital Personal Data Protection Act 2023 are among some of the most important legislation governing the use and processing of personal data on the internet today.

What stands out is how privacy matters not just because laws demand it, but because society depends on it. When artificial intelligence shapes daily life, information fuels predictions about what people will do, nudges their decisions, sometimes even steers conversations across communities. Such uses spark unease - over being subtly guided by unseen forces, over personal freedom fading, over too much control resting with those who hold massive amounts of collected details. Guarding private information then turns into a way to protect fair systems, block unfair treatment, make sure each person remains an independent thinker instead of reduced to

numbers stored somewhere.[9]

Conclusion

1. Summary of Findings

Examining how the use of AI is related to online tracking and regulation in place to protect an individual's personal information brings about questions about the very nature of privacy in contemporary society. Today we are going beyond simply recording information and are witnessing the process of the use of intelligent algorithms to sift through behavior, predict actions, incrementally. Traditional concepts about individuals being in control of their choices quickly diminish as computers do the decision-making. This technology observes behavior across broad networks. It doesn't simply gather data, it analyses them. Record-keeping transforms into predictions that influence the outcome without conscious human thought. It's normal to observe, often in an unperceivable way and to lose a degree of control over our information stream. The current legislation designed to be long-term cannot possibly adapt to rapid technological advancements in this area. Automated decisions affect opportunity before action is ever taken. In fact, current regulations created with longevity in mind struggle to cope with the sophistication of AI. Regulations such as the General Data Protection Regulation codify user rights, necessitate transparency, limit data use, and inhibit non-human decisions. Nevertheless, even the clearest legislations may find agreement on clarity with the code is lacking, especially across different countries and when the supervisory process disappears at the border. No area more starkly presents this rise of surveillance than the private and government sectors of society with technology such as facial scanning, data tracking and predictive policing. Driven by artificial intelligence, these methods have quietly become common. People worry about constant watching shaping what others say. Freedom to speak without fear starts shrinking when observation feels endless. Personal control over information fades as systems gather details without asking. What once felt private now flows into unseen databases. Across the globe, rules around data aren’t built the same way. In Europe, laws rest on protecting people’s core rights first. Meanwhile, places such as the U.S. shape policy by industry, leaning into market forces - patchwork results often follow.

[9] **The Age of Surveillance Capitalism**, Shoshana Zuboff (2019)

Bibliography

Books

- Solove, Daniel J., *Understanding Privacy* (Harvard University Press, 2008)
- Kuner, Christopher, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2020)
- Bygrave, Lee A., *Data Privacy Law: An International Perspective* (Oxford University Press, 2014)
- Edwards, Lilian & Veale, Michael, *Rewriting the Law for the Digital Age* (Hart Publishing, 2020)
- Hildebrandt, Mireille, *Law for Computer Scientists and Other Folk* (Oxford University Press, 2020)

Websites

- Ministry of Electronics & Information Technology (MeitY), Government of India
  https://www.meity.gov.in
- Digital Personal Data Protection Act, 2023 – MeitY Resource Page
  https://www.meity.gov.in/data-protection-framework
- Unique Identification Authority of India (UIDAI) – Aadhaar & Data Governance
  https://uidai.gov.in
- Supreme Court of India – Judgments & Case Information (Privacy, Surveillance, Fundamental Rights)
  https://main.sci.gov.in
- NITI Aayog – National Strategy for Artificial Intelligence (AI for All)
  https://www.niti.gov.in
- European Union Artificial Intelligence Act Overview
  https://artificial-intelligence-act.eu/
- Council of Europe – Data Protection
  https://www.coe.int/en/web/data-protection
- OECD AI Policy Observatory
  https://oecd.ai
- MIT Technology Review – AI and Privacy
  https://www.technologyreview.com

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618