MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

Right to Privacy and Data Protection: A Comparative Legal Analysis

Dr. Umesh Kumar, Assistant Professor
Bahra University, Waknaghat, Solan, Himachal Pradesh

Abstract

One of the most prominent legal and constitutional issues of the digital age has been the right to privacy and data protection. The collection, processing, storage and sharing of personal information have been transformed by information technology, artificial intelligence, social media platforms, and the advent of cloud computing and other developments. Governments, corporations, and digital intermediaries use personal data for a variety of economic, administrative and security-related activities on an ever growing scale. The advances in technology have improved communication and governance, but raised concerns about surveillance, unauthorised access, profiling, identity theft and unauthorised use of personal information. To address these challenges, laws and regulations have been adopted internationally to ensure privacy protection and accountability of data processors.

In this research article, the evolution of right to privacy and data protection has been analysed by making a comparative study of important jurisdictions of European Union, USA, India and some selected international legal instruments. It discusses the constitutional protection, legislation, judicial decisions and regulation related to informational privacy and personal data governance. The attention is paid to the European Union's General Data Protection Regulation (GDPR), the sectoral laws for privacy in the United States and the Digital Personal Data Protection Act, 2023 of India.

The article then examines the issues of cyber security, digital surveillance, artificial intelligence, biometric gathering data and cross border data transfers in the modern era. It requires the cooperation and adjustment of international norms that enable technological evolution, without compromising on human dignity and individual autonomy. The study ends with the conclusion that privacy and data protection are not only individual rights but an integral part of democracy, regulation of the digital economy and human rights jurisprudence in the twenty-first century.

Keywords: Right to Privacy, Data Protection, GDPR, Digital Personal Data Protection Act, Informational Privacy, Human Rights, Cyber Law, Surveillance, Artificial Intelligence, Comparative Law

Introduction

The right to privacy has always been identified as a part of human dignity, autonomy and freedom. In the past, privacy has been associated with “privacy from others”, which is the privacy against physical invasion in an individual's life. With the increasing use of electronic communication systems and digital technology, however, the definition of privacy has changed greatly[1]. To modern people, privacy is the right to informational self-determination, to control information about oneself, the right to confidentiality of communications and a right to be free of unwarranted surveillance.

With the advent of the internet economy, personal data has become an important economic asset. Social networking, e-commerce, financial institutions, health care providers, and governments collect vast amounts of information about individuals' identities, preferences, activities and biometric information. There are significant concerns about how this huge amount of personal data is being collected and processed, and how it could be misused, manipulated, discriminated against, and affect the rights of civil liberties. International documents that are the historical foundation of the legal recognition of privacy as a fundamental human right are: the Universal Declaration of Human Rights of 1948 (Article 12) and the International Covenant on Civil and Political Rights of 1966 (Article 17)[2]. These provisions ban on arbitrary interference with privacy, family, home and correspondence. With time, these protections have been broadened to also include the right to privacy in the digital sphere, through the constitutions and legislatures of various countries.Data protection law is a specific part of privacy law, which covers lawful processing of personal data. Data protection law does not aim at preventing data from being accessed by others, as privacy law does, but, instead, lays down procedural requirements for data controllers and processors[3]. These duties include consent, duties of security guards, transparency and remedies in cases of violations.There are various ways jurisdiction has reacted to privacy and data protection issues. From the EU perspective, privacy and data protection are considered fundamental rights and a comprehensive regulatory framework has been created with GDPR[4]. The U.S. has adopted a sector-specific approach with a focus on consumer protection and market regulation. The Digital Personal Data Protection Act, 2023, is a recent act passed in India following the Constitution's judgment in Justice K.S. Puttaswamy v. Union of India, which has established privacy as a fundamental right. The various approaches are very different with respect to philosophies of law, enforcement strategies and priorities of the regulations.

The article does comparative analysis of privacy and data protection laws to get an insight into the conceptual basis, the legal framework, judicial developments and current issues.

Conceptual Framework of Privacy and Data Protection

Meaning and Nature of Privacy: The word 'privacy' has no one, clear meaning. The concept of privacy has been variously defined in social, technological, and constitutional terms. Samuel Warren and Louis Brandeis were the ones who coined the phrase “the right to be let alone,” which epitomized privacy. Today, informational privacy, decisional autonomy and communication confidentiality are also considered types of privacy.

Informational privacy is the right of an individual to control the collection, use, disclosure, and storage of his or her personal information. The importance of this aspect has increased due to the digital era, in which personal information can be quickly processed and sent around the world at low costs.

Privacy is also of constitutional importance as it serves to guarantee liberty of individuals from too intrusive government interference[5]. Democracy societies consider privacy as vital to freedom of expression, freedom of association and political activity. If there is no privacy protection, then people can suffer from chilling effects on their personal and intellectual freedom.

Concept of Data Protection: Data protection is the legal, technological and institutional rules and regulations that set limits on the collection, processing, storage, transmission and use of personal data. In digital era, governments, businesses and digital platforms have become more and more able to access personal data as a valuable resource. If you're using social networks, on-line banking, searching for healthcare, on-line shopping, on-line studying, or on-line conversations, you're shedding tons of personal info[6]. The confidentiality of such information thus has become a major legal and ethical issue globally.

The aim of data protection law is to make sure that there is a lawful, fair, transparent and secure handling of personal information. It establishes standards that organisations and institutions have to adhere to when amassing or processing personal information, and it grants people rights that they have over their personal information. The idea of data protection law is to strike a balance between the promotion of technological innovation, economic growth, administration efficiency and the protection of the individual dignity, autonomy and privacy.

Data protection is intrinsically linked with the general notion of informational privacy. Informational Privacy is the person's right to control the collection, processing, sharing and retention of personal information by others. People often share their personal data with public institutions, private companies, banks, hospitals, companies and Internet service providers. The information might be misused for business, political, identification, discrimination, surveillance, and cybercrime purposes if not properly handled. Therefore, Data protection law is a protective mechanism that is aimed at preventing access to personal information which is unlawful or is being made in an inappropriate way.

---

[1] Mbah, G.O., 2022. Data privacy and the right to be forgotten. *World Journal of Advanced Research and Reviews*, *16*(2), pp.1216-1232.

[2] Kohl, U., 2023. The right to be forgotten in data protection law and two western cultures of privacy. *International & Comparative Law Quarterly*, *72*(3), pp.737-769.

[3] Huang, L., 2023. Ethics of artificial intelligence in education: Student privacy and data protection. *Science insights education frontiers*, *16*(2), pp.2577-2587.

[4] Solove, D.J., 2022. The limitations of privacy rights. *Notre Dame L. Rev.*, *98*, p.975.

[5] Ke, T.T. and Sudhir, K., 2023. Privacy rights and data security: GDPR and personal data markets. *Management Science*, *69*(8), pp.4389-4412.

[6] Islam, M.T., 2022. Legal Development for Privacy and Data Protection in Bangladesh. *Global Privacy Law Review*, *3*(4).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

Personal data typically refers to any information that is associated with a particular person, who is identified or identifiable[7]. An individual may be identified without the use of information such as their name, photograph, email address, biometric identifier or government identifier. Also, indirect identification is possible, such as through information derived from online identifiers, location data, IP addresses, behavior patterns and other information. With the development of new technologies, such as artificial intelligence and big data analytics, it is more likely than ever that someone can be identified, even from anonymised or partially anonymised data[8]. The amount of personal information has consequently increased significantly in the past few years.

Some information on the person is deemed to be especially sensitive and if disclosed or utilized, it can seriously affect the person. Personal data typically prevalent in sensitive access includes medical, genetic, biometric identifiers, financial, racial or ethnic origin, political opinions and beliefs, religious beliefs, sexual orientation and criminal history. The disclosure to or use of such information without the permission of the individual involved may result in a discriminatory effect, social exclusion, financial losses, damage to reputation, psychological harm or violation of fundamental rights. Consequently, some legal systems are more restrictive than others in the protection of personal data and impose higher compliance standards when it comes to sensitive data.

Data protection is now in a new avatar with digital technologies. The focus of privacy issues previously was mostly on physical intrusion or disclosure of confidential information without authorization. But today, digital ecosystems gather, track and analyze vast amounts of personal information via social media, cloud computing, wearable technology, surveillance systems, mobile apps and websites. Data is often called the “new oil” and is now being seen as a valuable economic asset in this digital world. Valuable user data includes targeted advertisements, consumer profiling, predictive data analytics and customized services for the technology companies. Governments also use data-driven governance systems to provide welfare, police, national security and governance. This is an efficient and innovative practice but also carries great risks in terms of mass surveillance, manipulation, profiling and loss of personal autonomy.

There are some fundamental principles that form the basis of lawful processing activities of data under data protection. These principles have been adopted in the international conventions, regional instruments and domestic laws of various jurisdictions. One of the fundamental principles is the principle of lawfulness, fairness and transparency. In accordance with this principle, personal data should be processed only for purposes which are legitimate, and in a lawful manner[9]. Persons need to be clearly informed about the nature, purpose and effects of data collection and processing operations. Organizations should avoid any practice that might be deceptive and/or misleading in the collection of personal information. The other basic principle is purpose limitation. This means that only for a specific, explicit and legitimate purpose, and not in a way that would change the purpose of the collection, personal information should be collected. For example, if a person's personal information is collected to treat their illness, the collection of that information should not be used for commercial advertising of other products or services without the proper legal consent, or the consent of the person. How to avoid the unnecessary and arbitrary use of personal information is called purpose limitation. Data minimisation suggests that companies only gather the minimum data that's required to accomplish the specific purpose. Users are exposed to data misuse, unauthorised access and data security breaches if there is too much and too much of personal data are collected. Therefore, the data collection in the institutions should not be indiscriminate and unlimited. The concept of the storage limits is related: Personal data must not be kept indefinitely. Information should be kept only for as long as necessary to fulfil the purpose for which it has been collected and/or gathered and for which it is intended by law.

The other major principle of data protection is accuracy. It is the duty of organizations that handle personal data to make sure data is accurate, complete and up to date. Unfair decisions in the workplace, health care benefits, financial services, or governmental benefits can be due to bad or stale data. As a result, people may be allowed to ask for their incorrect information to be corrected or rectified.The principles of integrity and confidentiality highlight the need to safeguard personal data from unauthorised access, loss, destruction and cybers attacks. To ensure the data security standards, it is vital to implement suitable technical and organizational measures, such as encryption, access controls, authentication methods and cybersecurity protocols. In recent years, the banking sector, health care and social media have endured major data breaches, and the consequences of not securing data is dire[10].

The most important recent development in contemporary data protection law has been the concept of accountability. While it is a part of the legal obligation to be compliant with the law, they should be able to demonstrate their compliance with the law through: The idea behind this is that instead of reacting to violations, the responsibility for data controllers and processors is to take proactive steps to comply with the law.

In addition to these obligations, data protection law provides a number of key rights for people about their personal data. Typically, these rights include access to your data, rectification, erasure or the right to be deleted, objection to certain data processing, portability and withdrawal of consent. These rights help to promote personal autonomy and the individual's control over the use of their information. In certain jurisdictions there is also a right to object to automated decision making systems and algorithmic profiling.Each country has taken on different strategies to data protection regulation. The EU has taken a rights-based approach to regulation with data protection defined as a fundamental human right, as stated in the General Data Protection Regulation (GDPR). The GDPR is very detailed and prescriptive and has “heavy” requirements for organisations, and a strong enforcement framework with substantial fines. In the USA, the approach is sectoral, with varying degrees of privacy protection in each sector. Recent developments in India has led to the enactment of the Digital Personal Data Protection Act, 2023, which provide a structured framework for personal data governance in the backdrop of increased digitalisation and constitutional recognition of privacy rights in India.Despite significant advances in the law, there are still many issues concerning data protection in the modern world. New technologies for data collection and surveillance, including artificial intelligence, facial recognition, cross-border data transfers, cloud computing and IoT devices, are able to collect data and monitor people without being covered by existing legal frameworks. Moreover, the balance between privacy and national security, business innovation and law enforcement needs is often quite precarious[11]. The legal landscape must continually adjust to the evolution of technology and the ways it is used.

International Legal Framework on Privacy and Data Protection: Concern for privacy and personal data has increasingly become a fundamental part of international human rights law. The increased digitalisation of technologies, world-wide means of communication, electronic commerce and trans-national data transfers has raised the issue of international law that can safeguard individual privacy on an international level. Important contributions to principles and norms on privacy and data protection have come from international organisations, regional institutions and multilateral agreements. While the approach taken by countries differs, there are also a number of international instruments which have set standards (whether through legislation or judicial interpretation) that affect the approach taken internationally. The concept of international law of privacy has developed based on the awareness that privacy is not only a private matter but is one of the means that define human dignity, freedom and democratic society. International legal documents seek to balance people's human rights and the legitimate rights and interests of the state, including those of the nation in the areas of national security, public order and economic development. Over the years, the definition of privacy has advanced from privacy against physical intrusion, to informational privacy, electronic communications, digital surveillance and the control of personal data.

Universal Declaration of Human Rights, 1948: One of the oldest and most important international human rights instruments that explicitly mentions the right to privacy is the Universal Declaration of Human Rights (UDHR) adopted by the United Nations General Assembly in 1948. The Declaration was adopted after World War Two, when the international community wanted to find universal principles to protect human dignity and freedom from arbitrary government action and authoritarianism. Article 12 of the UDHR explicitly provides for the right to privacy, which every person has: No one shall be subject to any arbitrary interference with his right to privacy, family, home or correspondence, nor to any attacks upon his honor and reputation[12]. It also asserts that each person is entitled

[7] Bakare[1], S.S., Adeniyi, A.O., Akpuokwe, C.U. and Eneh[4], N.E., 2024. Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations.

[8] Yanamala, A.K.Y. and Suryadevara, S., 2024. Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. *Revista de Inteligencia Artificial en Medicina*, *15*(1), pp.113-146.

[9] Vukovic, J., Ivankovic, D., Habl, C. and Dimnjakovic, J., 2022. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. *Archives of Public Health*, *80*(1), p.115.

[10] Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W., 2022. Digital technologies: tensions in privacy and data. *Journal of the academy of marketing science*, *50*(6), pp.1299-1323.

[11] Juma, I. and Faturoti, B., 2025. Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice. *International Review of Law, Computers & Technology*, pp.1-26.

[12] Yanamala, A.K.Y. and Suryadevara, S., 2023. Advances in data protection and artificial intelligence: Trends and challenges. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), pp.294-319.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

to the legal protection against such interference and/or attacks. This measure provided for privacy rights as a basic universal human right for all humans, regardless of nationality, race, religion or political affiliaton. The UDHR is not a treaty, but it has a tremendous moral, political and legal value. The provisions of this document have been quoted as a source of inspiration for many constitutional systems, judicial decisions and international agreements. With Article 12, the principles of modern privacy law were laid down in basics; it was about protecting privacy against arbitrary interference by the state and others.

With the advancement of technology the importance of the UDHR grew significantly. The Declaration's framers were thinking of the usual types of intrusion, such as an unauthorized search or eavesdropping on the telephone calling tree, but in modern times, the concept of privacy has expanded to include new forms of intrusion – electronic surveillance, wiretapping, interception of electronic communications, collecting personal data without prior consent, and digital profiling. Thus, Article 12 still holds great relevance in today's digital age.The Declaration also helped to bring privacy into the field of the international human rights.The Declaration also introduced privacy as a topic for international human rights for the first time, besides as a constitutional principle in one's own country. Since 1948 many national constitutions have embraced the following UDHR principles on privacy. A number of countries' courts have referred to the Declaration as a reference in their interpretation of guarantees of personal liberty and human dignity under their respective constitutions.

International Covenant on Civil and Political Rights, 1966: The International Covenant on Civil and Political Rights of 1966 (ICCPR) was adopted in 1966 and came into force in 1976, which took the privacy principles of the UDHR and added them to legally binding international obligations for state parties. The ICCPR is one of the most applicable international human rights conventions, and provides the most specific protection of civil and political liberties.

The right to respect for privacy, family, home and correspondence is explicitly enshrined in ICCPR in Article 17[13]. It also makes sure individuals are not the victims of any unlawful assaults on their honour and reputation. The Article creates a legal duty on states to provide effective legal protection from such interference.

Article 17 is much broader and more successful than Article 12 of the UDHR, and sets treaty obligations for states that ratify it. The provision doesn't allow arbitrary interference or unlawful interference. This distinction is crucial because of the possibility that there is some legitimate interference but it might still be a breach of the Covenant if it is unreasonable, disproportionate, and unnecessary in a democratic society.Article 17 has been of major concern for the United Nations Human Rights Committee, which keeps an eye on the implementation of the ICCPR. The Committee has reiterated that, beyond the physical context, privacy may also be respected in digital communications, electronic records and information systems, as well as in judicial decisions, in General Comments. The Committee has consistently expressed its concerns regarding the lack of legal protection for practices of surveillance, interception of communications and collection of data by States. Today, Article 17 is understood in the context of providing safeguards against unauthorized digital surveillance, against mass data collection, cyber monitoring and against intrusive technologies. Surveillance is only legitimate when performed legally, when it is necessary and when it is proportionate. Procedures should also be put in place to prevent abuse by the use of surveillance measures which could be arbitrary.The ICCPR has influenced in various ways the constitutional court and constitutional change in several jurisdictions. Article 17 is frequently used in the area of private rights, particularly those regarding telecommunications surveillance, surveillance of the Internet, information privacy[14]. The Covenant has thus gone on to serve as a vital source of international privacy law in democratic and developing legal systems.

European Convention on Human Rights: The European Convention on Human Rights (ECHR) was adopted in 1950 within the framework of the Council of Europe, and is one of the most sophisticated regional human rights documents on privacy protection. Article 8 of the Convention states the right to respect for private and family life, home and correspondence. Everyone has the right to respect for private and family life, home and correspondence is guaranteed under article 8[15]. It also declares that public authorities may interfere with the enjoyment of this right only in accordance with the law and when required in a democratic society in respect of matters of national security, public safety or in order to prevent crime or the infringement of the rights and freedoms of others.

The European Court of Human Rights (ECtHR) has broadly interpreted Article 8 and has made it a dynamic and developing privacy protection mechanism. The Court has taken a wide view of the term “private life”, encompassing personal identity, sexual orientation, reputation, autonomy over the body, environmental privacy, digital communications and informational privacy. The proportionality principle is one of the most important developments of the ECtHR. All interference must meet three criteria: legality, legitimate aim and necessity in a democratic society. Governments need to show that the limitation of privacy is proportionate to the purpose and has effective protections against misuse. The Court has rendered several pivotal decisions relating to surveillance and telecommunications. In Klass v. Germany, the Court acknowledged that secret surveillance measures can be justified for state security purposes, but stressed the importance of safeguards. The Court in Malone v United Kingdom ruled that there was no clear legal framework for the interception of telephones, and such an operation was in violation of Article 8. Recent cases have been concerning internet monitoring, biometric data bases, data retention policies and mass surveillance systems.

The ECHR has had a major impact on European privacy law, such as the General Data Protection Regulation (GDPR). A rights-based perspective on data protection is the common denominator of European legal systems: Privacy is regarded not as a tool to bring about policy or organizational changes, but as a fundamental human right, inextricably linked with dignity and autonomy of the individual.

OECD Privacy Guidelines: The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was adopted by the Organisation for Economic Co-operation and Development (OECD) in 1980. These guidelines were one of the earliest international initiatives to set out the harmonized rules on personal data protection in the light of computerization and increased globalization. The OECD acknowledged that more cross-border data flows would provide economic opportunities, but also presented a significant concern about how this personal information might be misused[16]. The Guidelines aimed to strike a balance between the freedom of information and privacy protection.The OECD Guidelines set out several principles which remain relevant today in the current data protection landscape. The principles include: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.The concept of collection limitation is that personal data should be collected in a lawful and fair way and if applicable, with knowledge or consent of the person[17]. The data quality principle focuses on the accuracy, completeness, and relevance of personal data that is used for a specific purpose.

When data is collected, purpose specification is a process in which the reasons for data collection are clearly identified. Limitation means that there is a restriction on disclosure or processing of personal data for another purpose than that for which it was originally disclosed or processed, if there is no consent or legal basis.

The security safeguards principle demands that organizations ensure that personal information is not accessed, used, disclosed, destroyed or altered without permission. The openness principle encourages transparency about data processing policies and data processing practices. Individual participation allows for access to and correction of personal information.The most important contribution of OECD Guidelines is the idea of accountability, or the requirement of data controllers to ensure compliance with their privacy obligations. This concept was later incorporated into contemporary standards like the GDPR[18].

The OECD Guidelines are not binding, but they are widely influencing the global privacy laws. The Guidelines are reflected in many national laws, regional instruments and also international agreements. They also helped to establish international consensus on fair information practices and responsible data governance.

Evolution of EU Privacy Law: The EU has one of the most extensive data protection regimes in the world. The right to privacy and data protection are enshrined in the Charter of Fundamental Rights of the European Union as a fundamental right (Articles 7 and 8).

---

[13] Oluoha, O.M., Odeshina, A.B.I.S.O.L.A., Reis, O.L.U.W.A.T.O.S.I.N., Okpeke, F.R.I.D.A.Y., Attipoe, V.E.R.L.I.N.D.A. and Orieno, O., 2023. A privacy-first framework for data protection and compliance assurance in digital ecosystems. *Iconic Research and Engineering Journals*, *7*(4), pp.620-646.

[14] Mantelero, A., 2022. Beyond data. In *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (pp. 1-43). The Hague: TMC Asser Press.

[15] Rachovitsa, A. and Johann, N., 2022. The human rights implications of the use of AI in the digital welfare state: Lessons learned from the Dutch SyRI case. *Human Rights Law Review*, *22*(2), p.ngac010.

[16] Jaime, F.J., Muñoz, A., Rodríguez-Gómez, F. and Jerez-Calero, A., 2023. Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, *23*(21), p.8944.

[17] Zhang, D., Finckenberg-Broman, P., Hoang, T., Pan, S., Xing, Z., Staples, M. and Xu, X., 2025. Right to be forgotten in the era of large language models: Implications, challenges, and solutions. *AI and Ethics*, *5*(3), pp.2445-2454.

[18] Bak, M., Madai, V.I., Fritzsche, M.C., Mayrhofer, M.T. and McLennan, S., 2022. You can’t have AI both ways: balancing health data privacy and access fairly. *Frontiers in genetics*, *13*, p.929453.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

In 1995 a harmonised legal framework (Data Protection Directive) was provided for member states. In 2016, however, the General Data Protection Regulation was enacted, as technology advances and globalization has made the need for increased regulation more evident.

General Data Protection Regulation (GDPR) GDPR was implemented in 2018 and revolutionized privacy laws around the world. It covers not only the organisations inside the European Union, but also those outside the European Union which process the data of EU residents[19].

Under the GDPR, there are a number of rights that a data subject has, such as the right to access, rectification, erasure, restriction of processing, data portability and the right to object to automated decisions[20]. Organisations must get valid consent, take reasonable steps to protect privacy when designing products and services, designate data protection officers under specific conditions and notify of data breaches as soon as possible.

The enforcement mechanism is one of the most important aspects of the GDPR. Administrative penalties for violations by supervisory authorities can be very high. This is a strength of regulation that has led multinational organisations to embrace global privacy compliance.

Judicial Interpretation in the EU: The role of the Court of Justice of the European Union has been crucial in boosting privacy safeguards. However, decisions like Google Spain v. AEPD gave rise to the "right to be forgotten" and allowed the removal of some search engine results. Likewise, Schrems I and Schrems II rendered data transfer agreements between the EU and the USA invalid because of an inadequate level of privacy protection.

United States Approach to Privacy and Data Protection

Constitutional Foundations: Data protection is not a separate fundamental right in the USA, as it is in the EU. Privacy protections come from the constitutional amendments, judicial interpretations, and statutory protections. The Fourth amendment safeguards against unreasonable searches and seizures, and the First amendment guarantees freedom of speech and association. These have been interpreted to cover some privacy rights by judicial decisions.

Sectoral Regulatory Model: The U.S. has a fragmented and sector-specific approach to privacy regulation. Various laws apply to various industries including the health and medical field, financial services, telecommunications, and even children's privacy.

Medical data is governed by the Health Insurance Portability and Accountability Act and financial data is governed by the Gramm-Leach-Bliley Act. The Children's Online Privacy Protection Act (COPPA) safeguards information about children.

This sectoral approach gives flexibility, but can lead to gaps and inconsistencies in regulation. The lack of a comprehensive federal privacy law is said to make consumers less protected and easier to comply with.

California Consumer Privacy Act: The California Consumer Privacy Act of 2018 was enacted by the state of California to expand consumer privacy rights. Legislation provides rights to access, delete and opt out of data sales. It has played a role in the debates on comprehensive federal privacy reform in the United States.

Privacy and Data Protection in India

Constitutional Recognition of Privacy: However, during many years the Indian Constitution does not mention privacy as a fundamental right. But as time passed, the interpretation of the constitutional rights with regard to life and personal liberty was extended. Justice K.S. Puttaswamy in his landmark case, Justice K.S. Puttaswamy v. Union of India, declared privacy as a fundamental right inherent in dignity, liberty and autonomy[21]. The Supreme Court highlighted an issue of informational privacy and stated that the risks of "modern technology" and of "state surveillance" must be recognized.

Information Technology Act, 2000: In the absence of any comprehensive privacy legislation, the framework of privacy regulation in India had been predominantly hinged on the Information Technology Act, 2000 and rules made under it. These established criteria had limited requirements for personal data that was sensitive and cyber security procedures.

The framework, however, had been criticized for poor enforcement, fuzzy definitions and narrow individual rights.

Digital Personal Data Protection Act, 2023: The Government of India has introduced the Digital Personal Data Protection Act, 2023 to provide a comprehensive framework for managing personal data. The legislation is applicable to digital personal data processing within the nation and in some extra-territorial circumstances. The Act includes rights over access, correction, erasure, grievance redressal and nomination. It sets obligations on data fiduciaries to lawful processing, data security and reporting of data breaches. Even though it's important, it has triggered discussions about exceptions for government entities, international data transfers, and regulatory autonomy. Some critics say that the general exemptions in government regulations could weaken the protections for informational privacy.

Comparative Analysis of Privacy Regimes: Internationally, privacy and data protection laws are highly fragmented in terms of their constitutional traditions, political philosophies, economic priorities, and legal cultures. While a growing number of legal systems acknowledge the need for safeguarding personal data in the digital era, their concepts of privacy, the legal frameworks, and their methods of enforcement vary widely[22]. The three examples of governance of privacy and data protection that can be found in the European Union, the United States and India are three distinct avenues. These all have different levels of protection, policy intensity, and institutional accountability due to their different experiences and policy goals.

A comparative study of these systems highlights that privacy law is more than a mere technical regulatory system, but is also a manifestation of broader philosophical values on human dignity, individual liberty, economic growth, state authority and market control. The E.U. has a rights-based perspective, which considers privacy and data protection as human rights. The USA has a market oriented and sectoral approach, with a focus on innovation and commercial flexibility. India is a developing hybrid country which is trying to reconcile constitutional rights with digital governance and economic modernization.

Philosophical Differences: There are several key differences between the privacy regimes, including their underlying philosophy. The concept of privacy is different in various legal systems based on their constitutional traditions and priority.

European Union Approach: The European Union considers privacy and data protection as being embedded in the human right to dignity, autonomy and freedom in democratic society. The method is very much set in the constitutional tradition of Europe and the philosophy of human rights since the Second World War. In European societies, there were significant abuses of personal information under authoritarian regimes and in wartime during surveillance, therefore protection of individuals from arbitrary state and corporate actions became an important focus.

The concept of privacy in the European context is more than consumer protection or contractual rights. Rather, it's seen as a fundamental part of personality, autonomy, and the dignity of the human person. The right to privacy is explicitly referred to in Article 1 of the Charter of Fundamental Rights of the European Union, which also mentions the right to data protection (Article 8).

The philosophy of "rights" shapes the form and force of European data protection law. European regulation focuses on transparency, accountability, informed consent and personal control[23]. Personal data is treated as a part of a person's identity and not just an economic asset, which means that organizations that process personal data have wide-ranging legal duties.

The European attitude is also a sign of distrust of the unlimited commercial use of personal data. Data processing companies will have to justify data processing on the basis of necessity and proportionality, as will public authorities. Thus European law sets strict limits on surveillance, profiling, automated decision making and cross-border data transfer.

[19] Novelli, C., Casolari, F., Hacker, P., Spedicato, G. and Floridi, L., 2024. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, *55*, p.106066.

[20] Singh, B. and Kaunert, C., 2024. Integration of cutting-edge technologies such as internet of things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. *GLS Law Journal*, *6*(1), pp.13-20.

[21] Novelli, C., Casolari, F., Hacker, P., Spedicato, G. and Floridi, L., 2024. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, *55*, p.106066.

[22] Singh, B. and Kaunert, C., 2024. Integration of cutting-edge technologies such as internet of things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. *GLS Law Journal*, *6*(1), pp.13-20.

[23] Williamson, S.M. and Prybutok, V., 2024. Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*, *14*(2), p.675.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

The General Data Protection Regulation (GDPR) is the most obvious statement of this philosophy. It highlights the principles of data minimization, purpose limitation, privacy by design and accountability. There are robust rights granted to individuals, such as rights to access, rectification, erasure, portability, and objection to data processing activities.

United States Approach

The United States takes a market approach and sectoral approach in regards to privacy regulation as opposed to European nations. Constitutional individualism, free market economics and limited government intervention in commercial activity are all deeply entrenched in the American landscape of privacy law.

In the United States, the idea of preserving privacy is sometimes expressed in terms of consumer rights, contractual obligations, or safeguards against government interference and not through the general principle of human dignity. State power is limited in the American constitutional tradition, and the Fourth Amendment guarantees against unreasonable searches and seizures is a prime example.

Data protection is not a constitutional right in the United States, as it is in the European Union. Rather, the protections for privacy arise from federal laws, state laws, judicial rulings, and industry regulations. This fragmented legal structure is based on the principle that there is a need for each sector to be regulated in a different manner.

The American policy makers are generally focused on innovation, technological development and commercial flexibility. Too much regulation may be detrimental to economic growth and entrepreneurial activity. This leaves companies more freedom to gather and use consumers' information than in Europe.

Self-regulation and market mechanisms are also crucial to the United States. Consumers are often held to account for safeguarding their own interests in contracts, privacy policies, and by making choices in the market[24]. Some critics contend that this undermines consent as it is weakened as the users may sometimes be lacking in bargaining power or technical knowledge about the data processing practices.

Meanwhile, the American model has fostered rapid technological innovation and development of digital industries. Within this relatively loose regulatory setting, big technology firms sprang up. But worries about surveillance capitalism, data leaks and targeted advertising, and algorithmic manipulation have created a push for more robust federal privacy law.

Indian Approach

In India, the approach is hybrid where the constitutional human rights principles, goals of economic development and national governance all come into play. Indian privacy law is unique to the country, in that it is a fast-digitizing democracy with many developmental challenges and many inhabitants who rely on digital governance systems.

The concept of privacy was not originally incorporated in the Indian Constitution. The landmark ruling in Justice K.S. Puttaswamy v. Union of India, however, has laid the foundations of Indian privacy rights and law by identifying privacy as an integral right to life and personal liberty under Article 21 of the Constitution.

The Supreme Court stressed that Privacy is not just about keeping information private, but also about having control over your body and over your decisions[25]. The judgment was largely informed by principles from international human rights, and comparative constitutional cases.

Concurrently, Indian privacy law should be able to balance other related issues of economic growth, digital inclusion, welfare distribution, cybersecurity, and national security. An expanding digital economy, biometric identification systems, the financial technology industry and e-governance programs across India demand vast data processing infrastructure.

Thus, Indian privacy law tries to strike a balance between privacy and governmental goals and economic modernisation. The Digital Personal Data Protection Act, 2023 seeks to create a regulated regime for the governing of personal data while allowing for flexibility in the state's actions and policies in development.

Critics say existing Indian laws are too wide-ranging and give too many exemptions to government bodies, and that there are not enough protection from mass surveillance. Backers argue that a balanced system is needed to facilitate an economic revolution and digital governance in a developing economy.

Regulatory Structures

European Union Regulatory Framework

The GDPR is one of the most centralized and complete privacy regulations worldwide by the European Union. The Regulation is applicable and sets the same requirements for all organisations that deal with personal data in the member states.

GDPR is a horizontal approach, so it applies to all industries and sectors. It must adhere to fundamental principles and obligations of data protection, regardless of the sector in which a company functions — be that healthcare, finance, education, telecommunications or social media.

The GDPR also has extraterritorial effect. If organisations outside Europe process the personal data of a European resident they must comply. This has made the GDPR a global benchmark impacting privacy policies around the world.

The Regulation calls for the implementation of privacy by design, requires data protection impact assessments and mandates the designation of data protection officers in specific cases, as well as prompt reporting of data breaches[26]. The scope of such obligations is indicative of Europe's conviction that the regulatory philosophy should be strong on rights.

United States Regulatory Structure

The United States has a piecemeal and sectoral approach to regulation. There is no single comprehensive privacy law, rather separate laws cover various industries and types of personal data.

Examples include the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data, the Gramm-Leach-Bliley Act for financial data, and the Children's Online Privacy Protection Act (COPPA) for children's online privacy.

In addition, individual states have enacted their own privacy laws. California's Consumer Privacy Act is among the most impactful state privacy laws and provides consumers rights concerning access, deletion and opt-out options.

This disjointed structure can lead to inconsistencies in regulation and compliance. Multi-jurisdictional and multi-sector companies often face compliance challenges with overlapping and conflicting mandates.

Indian Regulatory Structure

The Digital Personal Data Protection Act, 2023 is an effort to establish a comprehensive national framework for the governance of personal data in India. The law regulates the use of personal digital data and imposes duties on data fiduciaries, as well as rights on individuals.

Consent, Data security, Breach reporting, Correction, Erasure and Grievance redressal are all part of the Act[27]. The Indian law, however, offers greater governmental exemptions and less procedural protections than the GDPR.

There has also been a concern about institutional independence and mechanisms of oversight. Subsequent laws, judicial rulings, and administrative interpretation and implementation will play a large role in the success of India's privacy regime.

Enforcement Mechanisms

European Union Enforcement

EU has robust enforcement powers with independent supervisory bodies in each member country. The regulatory authorities have investigative powers and can levy large fines for non-compliance.

---

[24] Cheng, L. and Guo, Y., 2025. Privacy protection on social media platforms: Overdisclosure of online behavioral data is labeling users. *International Journal of Digital Law and Governance*, *2*(1), pp.107-133.

[25] Chen, S., 2022. The Latest Interface: Using Data Privacy as a Sword and Shield in Antitrust Litigation. *Hastings LJ*, *74*, p.551.

[26] Alfawzan, N., Christen, M., Spitale, G. and Biller-Andorno, N., 2022. Privacy, data sharing, and data security policies of women's mHealth apps: scoping review and content analysis. *JMIR mHealth and uHealth*, *10*(5), p.e33735.

[27] Custers, B., 2022. New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, *44*, p.105636.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

The GDPR could see fines of up to millions of euros or a percentage of annual turnover worldwide. This has led to a tough standard that has forced multinational businesses around the world to establish extensive compliance programs.
EU system focuses on accountability and proactive compliance. In addition to complying with the law, organisations must also show how they comply by keeping records, conducting audits and having systems and procedures in place to ensure compliance.

United States Enforcement

Regulatory bodies like the Federal Trade Commission (FTC), state attorneys general and private lawsuits are key to American privacy enforcement. The FTC's main concerns are with consumer data in unfair or deceptive trade practices.
The success of enforcement efforts is significantly different in different industry segments and under different state legislation. Most of the time, privacy cases are settled, consent decreed, or class action lawsuits.
There does not exist a federal privacy authority with the scope of authority that is comprehensive.The lack of an overarching federal privacy authority can sometimes result in less consistency and coordination in enforcement.

Indian Enforcement

The enforcement mechanism in India is still a work in progress[28]. The Digital Personal Data Protection Act sets up a Data Protection Board to settle cases and penalties.
Institutional independence, technical expertise, procedural transparency and enforcement capacity, however, will be important determinants of the long-term effectiveness of the Board. There are lingering concerns about the need for both regulatory oversight and governmental influence.
Additionally, there are certain practical issues like low digital literacy, cybersecurity risks and the sheer volume of data processing operations in India that need to be addressed through the enforcement mechanism.

Contemporary Challenges in Privacy and Data Protection

Artificial Intelligence and Automated Decision-Making

AI systems heavily depend on large-scale data processing. Machine learning algorithms can yield discriminatory results, intrusive profiling, and black-box decision making. The legal landscape is already complex and for the most part, inadequate in dealing with algorithmic accountability and explainability.

Government Surveillance

State surveillance has increased as a result of national security and counterterrorism programs. Mass surveillance mechanisms like metadata collection, facial recognition, and interception of communication places questions of proportionality and constitutional protection.

Cross-Border Data Transfers

International data transfers are essential for global digital commerce. But with varying privacy requirements, there are legal questionmarks and conflicts. Proposals to tackle these issues include adequacy decisions, standard contractual clauses, and bilateral agreements.

Cybersecurity Threats

Personal information security remains at risk from data breaches, ransomware and identity theft. There is a need to put in place a robust technical and organizational protection framework that will prevent unauthorized access and financial damage to organizations.

Biometric Data and Facial Recognition

Fingerprint, iris and face recognition technologies are more prone to privacy threats as the biometric characteristic cannot be changed easily[29]. Lack of adequate protection in many legal systems for the processing of biometric information.

Need for Harmonized Global Standards

Considering digital communication's transnational character, increased global collaboration on privacy regulation is required. Multinational corporations are faced with compliance challenges and individual protections diminish due to divergent legal standards.
The harmonisation process needs to start with defining minimum global standards on consent, transparency, accountability, security safeguards and cross-border transfers. Interoperable privacy frameworks can be developed via the contributions of international organisations and regional institutions[30].
Meanwhile, harmonization should take into consideration cultural diversity, constitutional traditions and developmental priorities. Regulatory uniformity can be detrimental to national sovereignty and innovation capability.

Conclusion

Data protection and the right to privacy is now a crucial legal question in the digital age. The technological advances have completely shifted the dynamics between people, companies and governments and introduced personal data as a new factor in economic and political power. This has led to a series of attempts by legal systems around the world to create systems that protect informational autonomy while at the same time promoting innovation and governance.
The comparison shows that there are substantial differences between legal regimes. The GDPR has the strongest rights-based approach provided by the European Union, which focuses on dignity, accountability and comprehensive regulation. The United States has a sectoral, market-based and flexible approach, with some inconsistencies. India is a hybrid with a developing pattern shaped by constitutional privacy law and digital governance agendas.
Although there have been strides in legislation, there are still many issues to be addressed. New challenges to the effectiveness of the current legal framework arise in the fields of artificial intelligence, biometric surveillance, cybersecurity threats and cross-border data flows. The question of striking a balance between privacy, national security, economic development and technological innovation is a complicated and developing one.
The legal evolution of the future should take place on the bases of the reinforcement of the legal framework of the institutions, improvement of international cooperation, increasing awareness of the user about the rights and responsibilities of algorithms, and promoting awareness of the public about digital rights. The core values of democracy, human dignity and rule of law in the 21st Century cannot be divorced from privacy and data protection, not only as technical regulatory issues.

[28] Wan, Z., Hazel, J.W., Clayton, E.W., Vorobeychik, Y., Kantarcioglu, M. and Malin, B.A., 2022. Sociotechnical safeguards for genomic data privacy. *Nature Reviews Genetics*, *23*(7), pp.429-445.

[29] Labadie, C. and Legner, C., 2023. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), pp.16-44.

[30] Doss, H.D. and Mishra, A., 2024. The Internet of Things (IoT): A Cripple to Data Privacy and Security. In *Internet of Things Vulnerabilities and Recovery Strategies* (pp. 1-18). Auerbach Publications.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1447-1453

Reference list

Mbah, G.O., 2022. Data privacy and the right to be forgotten. *World Journal of Advanced Research and Reviews*, *16*(2), pp.1216-1232.
Kohl, U., 2023. The right to be forgotten in data protection law and two western cultures of privacy. *International & Comparative Law Quarterly*, *72*(3), pp.737-769.
Huang, L., 2023. Ethics of artificial intelligence in education: Student privacy and data protection. *Science insights education frontiers*, *16*(2), pp.2577-2587.
Solove, D.J., 2022. The limitations of privacy rights. *Notre Dame L. Rev.*, *98*, p.975.
Ke, T.T. and Sudhir, K., 2023. Privacy rights and data security: GDPR and personal data markets. *Management Science*, *69*(8), pp.4389-4412.
Ahmad, N., 2023. Data privacy issues and risks with sharing on social media: An inquiry. *Russian Law Journal*, *11*(4), pp.597-611.
Islam, M.T., 2022. Legal Development for Privacy and Data Protection in Bangladesh. *Global Privacy Law Review*, *3*(4).
Bakare[1], S.S., Adeniyi, A.O., Akpuokwe, C.U. and Eneh[4], N.E., 2024. Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations.
Yanamala, A.K.Y. and Suryadevara, S., 2024. Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. *Revista de Inteligencia Artificial en Medicina*, *15*(1), pp.113-146.
Vukovic, J., Ivankovic, D., Habl, C. and Dimnjakovic, J., 2022. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. *Archives of Public Health*, *80*(1), p.115.
Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W., 2022. Digital technologies: tensions in privacy and data. *Journal of the academy of marketing science*, *50*(6), pp.1299-1323.
Juma, I. and Faturoti, B., 2025. Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice. *International Review of Law, Computers & Technology*, pp.1-26.
Yanamala, A.K.Y. and Suryadevara, S., 2023. Advances in data protection and artificial intelligence: Trends and challenges. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), pp.294-319.
Oluoha, O.M., Odeshina, A.B.I.S.O.L.A., Reis, O.L.U.W.A.T.O.S.I.N., Okpeke, F.R.I.D.A.Y., Attipoe, V.E.R.L.I.N.D.A. and Orieno, O., 2023. A privacy-first framework for data protection and compliance assurance in digital ecosystems. *Iconic Research and Engineering Journals*, *7*(4), pp.620-646.
Mantelero, A., 2022. Beyond data. In *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (pp. 1-43). The Hague: TMC Asser Press.
Rachovitsa, A. and Johann, N., 2022. The human rights implications of the use of AI in the digital welfare state: Lessons learned from the Dutch SyRI case. *Human Rights Law Review*, *22*(2), p.ngac010.
Jaime, F.J., Muñoz, A., Rodríguez-Gómez, F. and Jerez-Calero, A., 2023. Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, *23*(21), p.8944.
Zhang, D., Finckenberg-Broman, P., Hoang, T., Pan, S., Xing, Z., Staples, M. and Xu, X., 2025. Right to be forgotten in the era of large language models: Implications, challenges, and solutions. *AI and Ethics*, *5*(3), pp.2445-2454.
Bak, M., Madai, V.I., Fritzsche, M.C., Mayrhofer, M.T. and McLennan, S., 2022. You can't have AI both ways: balancing health data privacy and access fairly. *Frontiers in genetics*, *13*, p.929453.
Novelli, C., Casolari, F., Hacker, P., Spedicato, G. and Floridi, L., 2024. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, *55*, p.106066.
Singh, B. and Kaunert, C., 2024. Integration of cutting-edge technologies such as internet of things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. *GLS Law Journal*, *6*(1), pp.13-20.
Williamson, S.M. and Prybutok, V., 2024. Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*, *14*(2), p.675.
Cheng, L. and Guo, Y., 2025. Privacy protection on social media platforms: Overdisclosure of online behavioral data is labeling users. *International Journal of Digital Law and Governance*, *2*(1), pp.107-133.
Chen, S., 2022. The Latest Interface: Using Data Privacy as a Sword and Shield in Antitrust Litigation. *Hastings LJ*, *74*, p.551.
Alfawzan, N., Christen, M., Spitale, G. and Biller-Andorno, N., 2022. Privacy, data sharing, and data security policies of women's mHealth apps: scoping review and content analysis. *JMIR mHealth and uHealth*, *10*(5), p.e33735.
Alfawzan, N., Christen, M., Spitale, G. and Biller-Andorno, N., 2022. Privacy, data sharing, and data security policies of women's mHealth apps: scoping review and content analysis. *JMIR mHealth and uHealth*, *10*(5), p.e33735.
Custers, B., 2022. New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, *44*, p.105636.
Wan, Z., Hazel, J.W., Clayton, E.W., Vorobeychik, Y., Kantarcioglu, M. and Malin, B.A., 2022. Sociotechnical safeguards for genomic data privacy. *Nature Reviews Genetics*, *23*(7), pp.429-445.
Labadie, C. and Legner, C., 2023. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), pp.16-44.
Doss, H.D. and Mishra, A., 2024. The Internet of Things (IoT): A Cripple to Data Privacy and Security. In *Internet of Things Vulnerabilities and Recovery Strategies* (pp. 1-18). Auerbach Publications.