Page 2502 - 2515

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Data Privacy and Protection in the Digital Age: A Comparative Study of European and Indian Legal Frameworks

HARSH VARDHAN SINGH*

ABSTRACT

This paper examines the legal and regulatory frameworks governing data privacy and protection in the digital age, undertaking a comparative study of the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023. As personal data has emerged as a valuable economic and social resource, questions concerning privacy, accountability, security, and regulatory oversight have gained substantial importance in contemporary legal discourse. The paper evaluates the principal features of both regimes, including consent-based processing, the rights granted to individuals, the obligations imposed upon data fiduciaries and controllers, and the mechanisms designed to ensure compliance. While both regimes demonstrate a shared commitment to protecting informational privacy and enhancing user control over personal data, important differences persist regarding territorial applicability, enforcement structures, institutional independence, regulatory penalties, and cross-border data transfer mechanisms. Through comparative legal analysis, the paper argues that although the Indian framework represents a significant development in establishing a structured data protection regime, certain areas require further refinement to achieve greater effectiveness and international compatibility, particularly the strengthening of regulatory institutions, the improvement of enforcement mechanisms, and the establishment of clearer standards governing international data flows. The paper ultimately advocates a multi-layered privacy governance model grounded in transparency, accountability, and greater harmonisation with evolving global data protection standards.

Keywords: *Digital personal data protection, General Data Protection Regulation, fiduciaries, legal regime, institutional independence, cross-border data transfer.*

I. INTRODUCTION

The rapid growth of digital technologies has significantly altered the manner in which personal information is created, obtained, processed, and utilised across societies. Personal data has become a valuable resource in the modern digital economy, driving business models,

* Author is a student at Amity University, Lucknow Campus, India.

 [ISSN 2581-5369]

innovation, and technological development. The expansion of social networking platforms, electronic commerce, financial technology services, cloud computing, and artificial intelligence has given rise to the constant compilation and processing of immense quantities of confidential data.[1] Consequently, concerns regarding privacy, surveillance, the misuse of personal data, and regulatory accountability have become increasingly significant in both national and international legal discourse.

As governments and regulatory institutions attempt to balance technological advancement with individual rights, data protection laws have assumed a central role in shaping digital governance frameworks. The increasing frequency of data breaches, the unauthorised processing of information, and concerns regarding digital surveillance have further highlighted the necessity of establishing comprehensive legal mechanisms capable of protecting personal information while simultaneously enabling economic growth and technological innovation.

In India, discussions surrounding informational privacy have gained substantial constitutional importance. The Supreme Court recognised privacy as a vital component of the fundamental right to life and personal liberty under Article 21 of the Constitution in its landmark ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). The Digital Personal Data Protection Act, 2023 was ultimately passed as an outcome of this constitutional recognition, which laid the groundwork for the formation of a dedicated legislative framework governing the protection of personal data.

On a global scale, the General Data Protection Regulation of the European Union, which became applicable in 2018, significantly influenced privacy governance worldwide by introducing comprehensive standards relating to consent, accountability, data subject rights, and regulatory compliance. Owing to its broad territorial scope and stringent enforcement mechanisms, the GDPR has emerged as a benchmark against which numerous national privacy frameworks are assessed.

Against this background, a comparative examination of India's Digital Personal Data Protection framework and the GDPR becomes important in order to evaluate their similarities, differences, regulatory challenges, and the evolving future of privacy governance in an increasingly interconnected digital world.

[1] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 34 (7th ed. 2021).

 [ISSN 2581-5369]

II. The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is one of the leading comprehensive legal frameworks governing data privacy and information security in the European Union.[2] Introduced with the objective of strengthening individual control over personal information, the regulation established a structured legislative instrument for the storage, use, and processing of personal data. The GDPR imposes extensive obligations upon organisations, businesses, and institutions handling personal information, irrespective of their geographical location, when dealing with the data of EU residents. By emphasising transparency, accountability, user consent, and data subject rights, the regulation has significantly influenced global approaches to privacy governance and digital regulation.

A. Core pillars of the GDPR

The GDPR is founded upon seven principal data protection principles.

B. Lawfulness, fairness, and transparency

One of the most important principles of the GDPR is that confidential data must be processed lawfully, fairly, and transparently.[3] Organisations cannot collect or process personal information arbitrarily; rather, they must establish a valid legal basis before engaging in data processing activities. Such legal bases may include legal obligations, contractual necessity, consent, or legitimate interests recognised under law.

Organisations must further be transparent and clearly communicate to individuals the type of information collected, the purpose behind its collection, the duration of storage, and the entities with whom such information may be shared. This principle strengthens informational autonomy by ensuring that individuals remain aware of how their confidential information is utilised.

C. Purpose limitation

The principle of purpose limitation requires organisations to collect personal information only for specific, clearly defined, and legitimate purposes. Data gathered for one purpose should not subsequently be utilised for unrelated purposes unless additional authorisation or legal justification exists.

This principle seeks to prevent the excessive exploitation of personal information and ensures that organisations maintain discipline regarding the scope of data usage. By restricting

[2] Regulation (EU) 2016/679, of the European Parliament and of the Council, 2016 O.J. (L 119) 1, pmbl. recital 1.
[3] Regulation (EU) 2016/679, art. 5(1)(a) & art. 6, 2016 O.J. (L 119) 35.

 [ISSN 2581-5369]

secondary uses of personal information, the GDPR attempts to reduce the risks associated with surveillance, profiling, and the unauthorised commercialisation of data.

D. Data minimisation

The GDPR emphasises that organisations should collect only the amount of information necessary to fulfil a specific objective.[4] The excessive or unnecessary collection of personal information increases privacy risks and creates greater vulnerability in the event of security breaches.

Data minimisation encourages organisations to adopt necessity-based collection practices rather than accumulating information merely because the technological capability to do so exists. This principle is particularly crucial in an era of artificial intelligence and digital platforms, in which large-scale data collection has become increasingly common.

E. Accuracy

Personal information processed by organisations must remain accurate, relevant, and up to date. Inaccurate or outdated information may adversely affect individuals by leading to incorrect decisions, discriminatory outcomes, or the denial of services.

Under the GDPR, organisations are expected to implement mechanisms allowing individuals to correct, update, or erase inaccurate information. Maintaining data accuracy enhances reliability within digital ecosystems while simultaneously protecting individuals from the harms associated with erroneous data processing.

F. Storage limitation

The principle of storage limitation restricts organisations from retaining personal information indefinitely.[5] Data should remain stored only for as long as it is needed to accomplish the original purpose for which it was gathered.

Long-term retention increases the possibility of misuse, unauthorised access, and security breaches. Consequently, organisations are expected to establish retention policies, periodic reviews, and deletion mechanisms that ensure unnecessary information is removed once its purpose has been fulfilled.

[4] Regulation (EU) 2016/679, art. 5(1)(c), 2016 O.J. (L 119) 35.
[5] Regulation (EU) 2016/679, art. 5(1)(e), 2016 O.J. (L 119) 35.

 [ISSN 2581-5369]

G. Integrity and confidentiality

To protect personal information, organisations must put in place the technical and organisational measures necessary to prevent unauthorised access, accidental disclosure, alteration, or destruction of data.

This principle places considerable emphasis upon cybersecurity measures, encryption techniques, access controls, breach reporting mechanisms, and internal security procedures. As digital infrastructure increasingly supports economic activities and governance structures, maintaining confidentiality and integrity has become essential for preserving trust within digital ecosystems.

H. Accountability

The accountability principle distinguishes the GDPR from many earlier privacy frameworks, because it requires organisations not only to comply with privacy obligations but also to actively demonstrate such compliance.[6]

Organisations must maintain documentation, establish internal privacy policies, conduct risk assessments, appoint Data Protection Officers where necessary, and create mechanisms capable of evidencing compliance before regulatory authorities. Accountability transforms privacy protection from a reactive approach into a proactive governance model, thereby strengthening institutional responsibility.

Collectively, these seven pillars form the normative foundation of the GDPR and provide an important framework for evaluating whether emerging data protection systems, including India's Digital Personal Data Protection framework, effectively protect confidential data in an increasingly digital society.

III. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is India's first comprehensive legislative measure specifically designed to regulate the collection, processing, use, and storage of digital personal information.[7] Enacted in response to growing concerns surrounding privacy, digital governance, and data misuse, the legislation seeks to establish a structured regulatory environment for personal data protection within an expanding digital economy. The framework attempts to strike a balance between safeguarding individual privacy rights and enabling organisations, businesses, and public authorities to process personal information for legitimate

[6] Regulation (EU) 2016/679, art. 24, 2016 O.J. (L 119) 46.
[7] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 4 (India).

 [ISSN 2581-5369]

and lawful purposes. By introducing obligations for data fiduciaries and rights for individuals, the Act marks a significant step toward strengthening India's evolving privacy and data governance regime.

The DPDP Act, 2023 is established upon seven core principles.

A. Consented, lawful, and transparent usage

One of the central features of the DPDP framework is that the processing of personal data must occur through lawful and legitimate means. Organisations, businesses, and entities processing personal information are expected to ensure that data collection serves lawful objectives and remains within the boundaries established by the legislation.

Transparency is equally important within this framework. Data fiduciaries are obliged to provide individuals with clear, accessible, and understandable notices explaining what personal information is being collected, the reasons for such collection, and how the information may be used. Such transparency strengthens informed decision-making and allows individuals to exercise greater control over their personal information.

Consent also remains a significant component of the framework. Individuals retain the authority to withdraw previously granted consent whenever they choose, thereby reinforcing autonomy and control over their personal information.

B. Purpose limitation

The principle of purpose limitation requires that personal information collected by organisations be utilised only for the specific objective communicated at the time of collection.[8] Information collected for one purpose cannot automatically be repurposed for unrelated activities.

This principle acts as an important safeguard against the misuse of personal information by preventing organisations from engaging in undisclosed secondary uses of data. Where organisations intend to process information for objectives beyond the originally communicated purpose, fresh authorisation or consent becomes necessary.

C. Data minimisation

The DPDP framework emphasises collecting only that personal information which is genuinely necessary for achieving a specified purpose. Organisations are expected to avoid the unnecessary accumulation of personal information simply because technological systems permit large-scale collection.

[8] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 6 (India).

 [ISSN 2581-5369]

Restricting collection practices to essential information reduces the risk associated with misuse, unauthorised access, and excessive surveillance. The prohibition against excessive or irrelevant data collection encourages organisations to adopt more responsible and proportionate data practices.

D. Accuracy of personal data

Maintaining accurate personal information forms another important component of the legislation.[9] Data fiduciaries are expected to take adequate steps to ensure that the information being processed remains correct, complete, and appropriately updated whenever necessary.

Accurate information reduces the possibility of individuals suffering harm due to incorrect records, outdated information, or inaccurate profiling. By imposing this obligation, the framework attempts to strengthen fairness and reliability within digital data ecosystems.

E. Storage limitation

The legislation discourages the indefinite retention of personal information by establishing limitations regarding storage duration. Personal information should not remain stored permanently unless legally required or justified for continuing purposes.

Organisations are expected to erase personal information once the need for which it was stored has been fulfilled, or when individuals withdraw previously granted consent. Such deletion obligations aim to reduce the unnecessary accumulation of personal information and minimise long-term privacy risks.

F. Reasonable security safeguards

Protecting personal information from unauthorised access, leaks, misuse, or accidental disclosure forms an essential obligation under the framework. Organisations processing personal information are expected to implement reasonable technical and organisational safeguards capable of preventing security breaches.

As digital transactions, cloud storage systems, and online platforms continue to expand, security safeguards become increasingly important for maintaining public trust and protecting sensitive information from cyber threats and unauthorised exploitation.

[9] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 8 (India).

 [ISSN 2581-5369]

G. Accountability

The DPDP framework places legal responsibility upon entities that determine the purposes and means of personal data processing.[10] Such entities remain accountable for ensuring compliance with statutory obligations and for maintaining responsible data governance practices.

The legislation also establishes an enforcement mechanism through the Data Protection Board of India, which is empowered to address grievances and investigate violations. Non-compliance, the failure to implement safeguards, or significant breaches may result in substantial financial penalties, extending up to 250 crore rupees in certain cases.

Collectively, these principles represent the foundational structure of India's evolving privacy framework and provide an important basis for comparative assessment with established international models such as the GDPR.

IV. Comparative analysis of the GDPR and India's Digital Personal Data Protection framework

Aspect	GDPR (European Union)	DPDP Act (India, 2023)
Territorial Scope	The GDPR adopts a broad territorial approach and applies not only within the European Union but also to organizations located outside Europe when processing data relating to EU residents. Its extraterritorial applicability makes it one of the most influential global privacy frameworks.	The DPDP Act primarily focuses on data processing activities connected with India and applies to entities processing digital personal information within Indian jurisdiction. Although it includes limited extraterritorial application, its scope remains comparatively narrower.
Consent Framework	GDPR places substantial emphasis upon informed, freely given, specific, and explicit consent. Organizations must clearly establish lawful grounds before processing personal information.	The DPDP Framework also recognizes consent as the foremost basis for processing but introduces certain circumstances where deemed consent may be permitted for specified lawful purposes.
Rights of Individuals	Individuals are granted extensive rights including access to confidential data, correction of inaccurate data, deletion rights, portability rights, and the ability to object to processing activities.	The Indian Framework provides individuals with rights relating to access, correction, grievance redressal mechanisms, and the ability to nominate representatives in certain situations.
Regulated Entities and Obligations	GDPR differentiates between data controllers and processors while imposing detailed compliance obligations upon both categories depending on their functions.	The DPDP framework established the concept of data fiduciaries and significant data fiduciaries, with regulatory obligations varying according to the nature and scale of processing activities.
Regulatory and Enforcement structure	Enforcement under GDPR is carried out through independent supervisory authorities across EU member states together with coordinated oversight mechanism at the European level.	Enforcement responsibilities under the DPDP framework are assigned to the Data Protection Board of India, though debates continue regarding institutional independence and regulatory autonomy.

[10] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 10 (India).

Penalty Structure	GDPR incorporates stringent financial consequences for violations, with penalties potentially extending to 20 million or 4% of global annual turnover depending upon the nature of non- compliance.	The Indian legislation prescribes monetary penalties that may extend up to 250 crores for specified violations, data breaches, and failures in compliance obligations.
Cross- Border Data Transfers	International data transfers under GDPR are governed through structured mechanism including adequacy decisions, contractual safeguards, and detailed compliance requirements.	The DPDP framework currently adopts a comparatively flexible approach toward international transfers but provides relatively limited guidance regarding operational standards and transfer mechanisms.
Underlying regulatory philosophy	GDPR strongly emphasizes informational self- determination, individual autonomy, accountability, and harmonized privacy governance across jurisdictions.	The DPDP framework attempts to balance privacy protection with economic growth, technological development, innovation, and digital governance objectives.
Overall approach to privacy governance	The European framework adopts a right-centric model prioritizing strong regulatory oversight and comprehensive compliance obligations	India's approach reflects a developing privacy framework seeking equilibrium between protecting personal information and enabling digital economy expansion.

Comparative analysis of the GDPR (European Union) and India's Digital Personal Data Protection framework.

A comparative assessment demonstrates that, while both frameworks share common objectives relating to privacy protection and responsible data governance, they differ significantly in regulatory structure, enforcement mechanisms, territorial reach, and institutional design.[11]

A. Challenges and gaps between the GDPR and the DPDP Act, 2023

Although both the GDPR and the DPDP Act, 2023 seek to strengthen privacy protection and regulate the use of personal information, important differences continue to exist in their structure, regulatory philosophy, and implementation mechanisms. These differences create multiple challenges when comparing the two frameworks, particularly regarding scope, enforcement, individual rights, and international data governance.

B. Differences in scope and applicability

One of the significant distinctions between the two frameworks lies in their scope of application.[12] The GDPR adopts a broader approach by regulating both digitally processed information and structured non-digital records containing personal information. In contrast, the DPDP framework primarily governs digital personal data and extends to physical information only when such data is digitised.

Another important gap relates to publicly available information. Under the Indian framework, personal information voluntarily made public by individuals, or through legally authorised

[11] COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS 12 (2018).
[12] *Id.* at 12.

disclosures, may fall outside certain protections. The European approach remains comparatively stricter by continuing to regulate personal information even when it becomes publicly accessible.

C. Variations in the legal basis for data processing

The GDPR establishes multiple legal foundations for processing personal information, including contractual obligations, legal requirements, legitimate interests, consent, and other recognised grounds. This flexibility allows organisations to process information without depending exclusively upon user consent.

The Indian framework, by contrast, places comparatively greater emphasis upon informed consent as the primary basis for processing activities. Although the legislation recognises certain legitimate uses, it does not create an expansive legitimate interest framework for private entities. As a result, organisations operating within the Indian system may rely more heavily upon consent-based mechanisms.

D. Differences in individual rights

Another major area of divergence concerns the rights available to individuals. The GDPR grants extensive protections, including rights relating to data portability and safeguards against decisions based solely upon automated processing systems.

The DPDP framework provides rights relating to access, correction, grievance redressal, and nomination, but does not explicitly provide similar protections concerning data portability or automated decision-making. Additionally, grievance procedures under the Indian framework generally require individuals to first approach internal grievance mechanisms before seeking regulatory intervention.

E. Enforcement structure and compliance challenges

The enforcement models adopted by the two frameworks differ considerably.[13] The GDPR creates direct responsibilities not only for controllers but also for processors involved in handling personal information. Under the Indian model, primary responsibility largely remains with data fiduciaries.

Similarly, data breach notification requirements vary. The European framework imposes specific reporting timelines and risk-based notification obligations, whereas the Indian system

[13] PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE 5 (2017).

 [ISSN 2581-5369]

generally requires communication regarding breaches to both regulatory authorities and affected individuals.

Another important difference concerns institutional structure. The GDPR functions through decentralised supervisory authorities operating across multiple jurisdictions, whereas the Indian framework centralises oversight through the Data Protection Board of India.

F. Cross-border data transfer challenges

The international transfer of personal information remains one of the most significant differences between the two systems. The GDPR follows a comparatively strict framework, permitting transfers primarily through adequacy mechanisms, contractual safeguards, and other recognised compliance instruments.

India's framework adopts a relatively more flexible model, permitting transfers to jurisdictions unless specifically restricted through governmental notifications. While this approach may support digital economic growth and business flexibility, it also raises concerns regarding the absence of clear and uniform standards for international data transfers.

V. CASE PRECEDENTS

A. The Meta fine of 1.2 billion euros (2023)

In May 2023, Meta was subjected to a financial penalty of 1.2 billion euros, making it the highest monetary sanction issued under the General Data Protection Regulation to date.[14]

The decision was issued by Ireland's Data Protection Commission, acting within the cooperation framework of the European Data Protection Board, reflecting coordinated regulatory oversight within the European privacy framework.

Regulators concluded that Meta had breached Article 46 of the GDPR by continuing to transfer the personal data of European users to the United States through the use of Standard Contractual Clauses, despite concerns regarding the adequacy of safeguards for such transfers.

In addition to imposing the monetary penalty, the regulatory authorities directed Meta to suspend further transfers of personal data to the United States and required the company to bring its data processing activities into compliance with the regulation, either by deleting the unlawfully transferred information or by relocating such data processing arrangements within legally permissible frameworks.

[14] Regulation (EU) 2016/679, art. 46, 2016 O.J. (L 119) 67.

 [ISSN 2581-5369]

B. Justice K.S. Puttaswamy (Retd.) v. Union of India

The development of India's data protection framework is closely connected with the landmark ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which recognised privacy as a fundamental right under Article 21 of the Constitution.[15] This decision became the constitutional foundation for later privacy reforms, including the Digital Personal Data Protection Act, 2023.

A nine-judge bench of the Supreme Court unanimously held that privacy is an essential aspect of personal liberty, dignity, autonomy, and individual freedom. The Court emphasised that privacy extends beyond physical space and includes informational privacy, which concerns the collection, storage, and use of personal data in an increasingly digital society.

The judgment acknowledged that rapid technological developments had created new challenges relating to surveillance, profiling, and the unauthorised use of personal information. Consequently, the Court recognised the need for legal safeguards capable of protecting individuals against arbitrary interference with their personal data.

Another significant contribution of the judgment was the articulation of the proportionality principle. The Court held that any restriction upon privacy must satisfy the tests of legality, necessity, and proportionality, thereby creating constitutional limitations on State interference.

The DPDP Act reflects several principles emerging from the judgment, including consent-based processing, accountability obligations, individual control over personal information, and safeguards against misuse. *Puttaswamy* therefore remains a foundational precedent that continues to shape India's evolving privacy and data governance jurisprudence.

C. Venkatesh Nayak v. Union of India (2026)

This matter represents one of the significant constitutional challenges to have emerged in relation to India's data protection framework. The case was initiated through writ petitions filed by activists and journalists questioning multiple provisions of the DPDP Act, as well as the subsequently notified DPDP Rules. A major concern raised in these petitions relates to section 44(3), which amends provisions of the Right to Information Act and is argued to create broad restrictions on the disclosure of personal information, thereby potentially reducing public transparency and citizen oversight. The petitions also challenge provisions concerning the composition and functioning of the Data Protection Board, raising concerns regarding executive

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

 [ISSN 2581-5369]

influence and the extent of the exemptions granted to the State. These issues are presently under consideration before the Supreme Court.

VI. Conclusion

The increasing dependence upon digital technologies has transformed personal information into one of the most valuable resources within contemporary society, making data protection an essential component of modern governance. The comparative analysis of the European Union's General Data Protection Regulation and India's Digital Personal Data Protection framework demonstrates that, while both legal systems pursue the common objective of protecting personal information and strengthening privacy rights, they adopt significantly different regulatory approaches.

The GDPR has emerged as a comprehensive and rights-oriented framework characterised by extensive individual protections, strong institutional enforcement mechanisms, strict cross-border transfer requirements, and accountability-based compliance structures. In contrast, India's DPDP Act, 2023 represents an important legislative milestone that seeks to establish a balanced framework capable of simultaneously protecting privacy while supporting innovation, digital growth, and economic development.

The analysis further demonstrates that, despite several similarities regarding consent, transparency, accountability, and lawful processing, important gaps remain concerning enforcement structures, institutional independence, individual rights, data portability, cross-border transfers, and State exemptions. Judicial developments, particularly the *Justice K.S. Puttaswamy* judgment, have played a foundational role in establishing informational privacy as a constitutional value and continue to influence India's evolving privacy jurisprudence.

Contemporary challenges involving technological expansion, artificial intelligence, global data flows, and increasing State and corporate access to personal information require privacy frameworks capable of adapting to rapidly changing digital environments. Therefore, strengthening institutional safeguards, improving regulatory clarity, enhancing enforcement mechanisms, and promoting greater alignment with international standards remain essential for creating an effective and sustainable privacy governance framework. Ultimately, achieving a balance between innovation, economic growth, and the protection of individual rights will determine the long-term success of modern data protection laws.

 [ISSN 2581-5369]

VII. BIBLIOGRAPHY

1. COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018).
2. EUROPEAN DATA PROTECTION BOARD, Reports and Publications.
3. IAN LLOYD, INFORMATION TECHNOLOGY LAW (Oxford Univ. Press, 9th ed. 2020).
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
5. PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE (Springer 2017).

*****

 [ISSN 2581-5369]