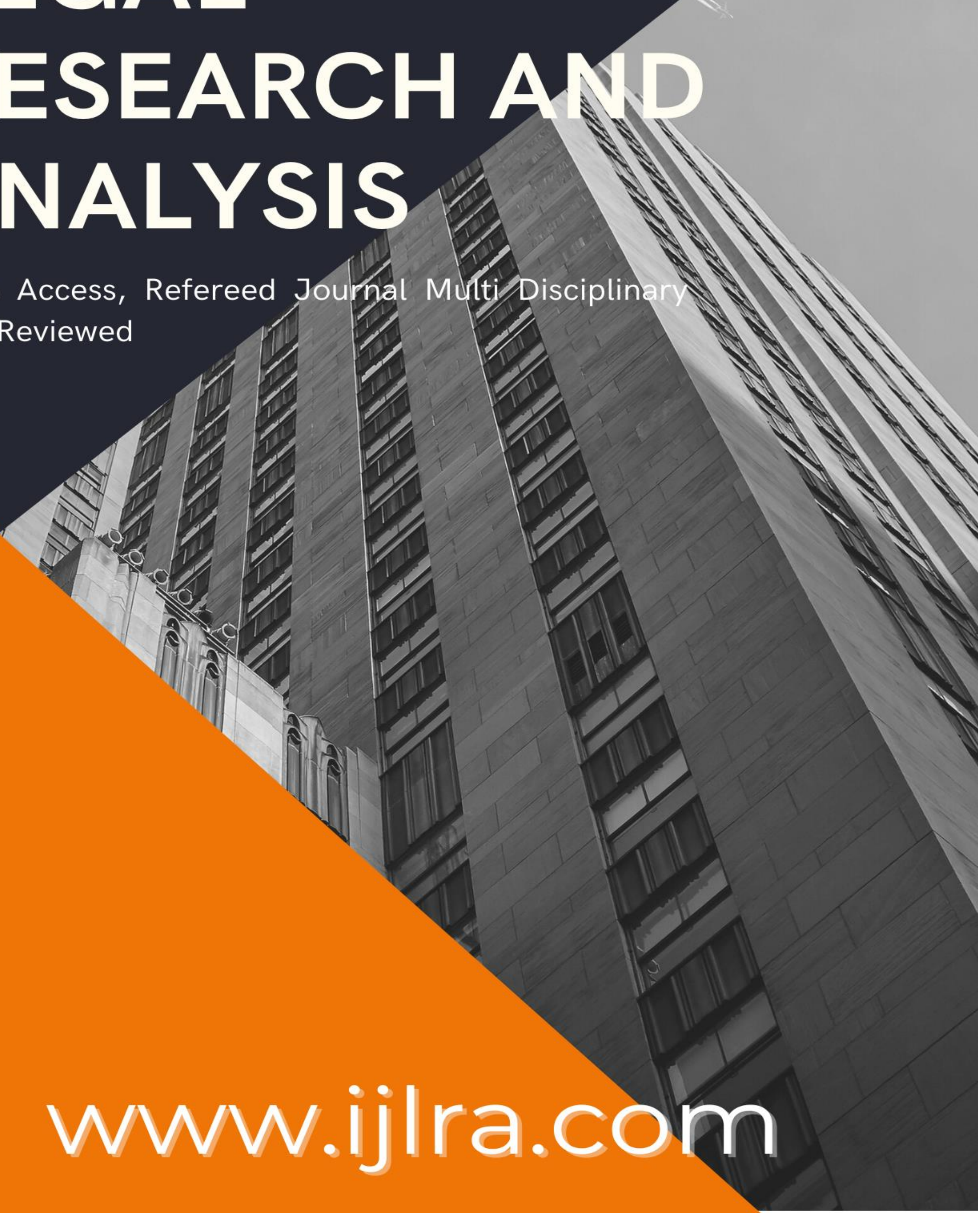
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DATA PROTECTION AND DIGITAL ECONOMY IN INDIA

AUTHORED BY - HASEEBA SHIFA

ABSTRACT

The expansion of digital technology in India has made personal information a critical issue in contemporary governance and economic activity. Digital platforms have transformed financial transactions, commercial services, communication, and public administration; however, their growing dependence on personal information has also intensified concerns about privacy, security, and accountability. The **Digital Personal Data Protection Act (DPDPA)** provides a legal framework intended to address these challenges and promote the responsible management of digital personal data. This paper critically examines the DPDPA by assessing its implications for individual privacy, organizational responsibilities, regulatory compliance, and India's digital economy. It further compares the Act with the **General Data Protection Regulation (GDPR)** to examine differences in individual safeguards, data governance, and institutional obligations. The study argues that the DPDPA is an important foundation for strengthening privacy protection in India, although its success will depend on effective implementation, regulatory oversight, organizational preparedness, and robust security practices. The paper concludes that sustainable data governance requires a careful balance between protecting individual privacy and enabling legitimate data use, technological innovation, and digital economic growth. The paper uses information from courts, laws, government policies, and schools. This information helps to see what is good about the privacy rules in India and what is not so good about the privacy rules in India. The study says that to really protect people's privacy in India, India needs institutions that're responsible. India needs companies that use data in a responsible way. India needs technology to keep information safe. The study says that India needs to find a balance between protecting people's privacy and using data. India needs to use data in a way so that people trust the world in India. This will help new ideas to happen, and the economy in India can grow. India needs to make sure that people's personal information is safe so that they can trust the world in India. The study concludes that privacy protection will be meaningful only when the legal framework is supported by effective implementation, capable authorities, and workable compliance measures. It calls for a balanced data policy that

protects individuals while allowing responsible information use, technological development, and economic growth.

Keywords: Data Privacy, Digital Economy, Cybersecurity.

INTRODUCTION

Data protection is an important foundation of the modern digital economy. Information collection, processing, sharing, and violation are only a few of the many actions that fall under the broad category of privacy. Both younger and older consumers seem to be growing increasingly concerned about privacy over time; however, older consumers' concerns seem to be growing more significantly. Half of the customers polled in an analysis said they would be less inclined to divulge personal information in the future. This research indicates that businesses are already preparing for less access to consumer-provided data, which makes more subversive data collection techniques appealing. The situation of internet users' online privacy has drastically changed in recent years. This year, the data security market will generate more than $7 billion in revenue, in 2024. The revenue is forecast to increase by 11.28% per year (CAGR) to over US$12 billion by 2029 (Statista Market Insights, 2024). Data flows are beneficial to consumers in the digital world on an economic basis. Use new services such as recommendations, search engines, special offers, ads, and targeted products and services.

Additionally, customized communication can help clients make well-informed decisions and reduce information overload. The question of which information sources are reliable is one that users of social media and Internet technologies are increasingly asking themselves. The need for privacy and data protection is becoming more widely acknowledged as more and more social and commercial activities take place online. Data protection aims to strike a balance between the benefits and risks of processing personal data, so that people can feel secure knowing that their information is collected, stored, and used only for appropriate purposes. The adoption of digital government and private-sector services, as well as investment, competition, and innovation in the digital economy, may be stimulated by a robust data protection framework that provides assurance (UNCDF, 2022). Digitalization of the economy has several goals and aims, which include advancing technology, increasing efficiencies, and improving services across the country. However, a productive transition to a digital economy is important for development and creates opportunities for more equitable and sustainable growth for overall improvement. The digital economy also helps with infrastructure and addresses policy

ISSN: 2582-6433

issues in several areas, including education, agriculture, government, finance, transportation, and climate. A data protection law aims to ensure that every individual's data is secure, safe, used fairly, and treated ethically and appropriately. It provides individuals' rights to control their own data, which includes the ability to access and provide consent for its use. It creates accountability for data processing, enabling adequate redressal mechanisms in the event of harm or damage. India has finally passed a data protection law after years of deliberations and consultations, as well as several attempts at legislation. Data protection aims to strike a balance between the benefits and risks of processing personal data, so that people can feel secure knowing that their information is collected, stored, and used only for appropriate purposes. The adoption of digital government and private sector services, as well as investment, competition, and innovation in the digital economy, may be stimulated by a robust data protection framework that offers assurance. Yet challenges like the digital divide, data privacy, and cybersecurity issues persist. Enhancing digital literacy and bolstering cybersecurity will play a major role in continued growth and in solving these problems as digital services continue to grow. The relationship between data protection and the digital economy is complex. Strong data-protection standards can increase consumer confidence, encourage responsible innovation, facilitate trustworthy digital transactions, and strengthen India's position in the global digital marketplace. At the same time, the heavy burden of regulation or uncertainty could present compliance issues, especially for start-ups, small and medium-sized organizations, or companies that heavily use data-based technologies. Therefore, India faces key challenges in creating a regulatory framework that safeguards individual rights while simultaneously fostering technological innovation, investment, market competition, and digital entrepreneurship. Data has become a vital asset in India's digital economy, supporting innovation, economic growth, and the delivery of digital services. At the same time, the increasing collection and use of personal information have made privacy, data security, and public trust more important for the sustainable development of the digital economy.

The Digital Personal Data Protection Act (DPDPA) of 2023 is the primary legislation in India for data privacy and protection. The following sections may be of interest to your study:

Section 4 – Scope of the Act

Section 6 – Consent for Processing Personal Data

Section 8 – Rights of Data Principals (Individuals)

Section 10 – Responsibilities of Data Fiduciaries (Organizations managing data)

Section 17 – International Data Transfers

Section 19 – Formation of the Data Protection Board of India

Section 25 – Penalties for Non-compliance

EVOLUTION OF DATA PROTECTION LAW IN INDIA

The increasing use of digital technology has created a new problem for individuals and organizations: how to keep personal information safe. Every day, people provide their details to banks, shopping websites, mobile applications, social media platforms, schools, hospitals, and other online services. Once this information becomes digital, it can be stored, transferred, and processed very easily. India has gradually developed laws to deal with privacy and security concerns connected with personal information.

The story began with the Information Technology Act of 2000. When this law was introduced, India was still at an early stage of Internet development. The country needed a legal system that could deal with electronic records, online transactions, and offences involving computers. The Act provided this foundation. It also dealt with certain situations involving confidential information and its unauthorized disclosure. However, it would be incorrect to describe the Act as a complete personal data protection law. Its broader purpose was to provide legal recognition to electronic activities and address the problems that came with the use of computers and digital communication.

With the expansion of the Internet, the nature of the problem changed. Organizations began to collect large amounts of information about their customers and users. This created concerns that went beyond cybercrime. People became interested in knowing what information was being collected about them, why organizations needed it, and what happened to that information after it was collected. Privacy consequently became a much bigger part of the discussion about India’s digital future.

In response, the Justice B.N. Srikrishna Committee was established in 2017. Its task was to examine India’s data protection requirements and suggest an appropriate legal framework. The Committee submitted its report in 2018, titled *A Free and Fair Digital Economy*. The report emphasized the individual’s interest in personal information while also recognizing the practical value of data. Modern businesses depend on information to provide services and make decisions, researchers use it to conduct studies, and governments may need it for various public purposes. The Committee therefore considered how privacy could be protected without making legitimate use of data impossible.

The recommendations were followed by the Personal Data Protection Bill, 2019. The proposed legislation attempted to create a dedicated system for dealing with personal data. It proposed a Data Protection Authority and included provisions intended to give individuals greater control over information concerning them. The Bill dealt with matters such as obtaining consent, dealing with complaints, transferring personal data, and requesting the removal of certain information.

The proposal did not ultimately become law. In 2022, the Personal Data Protection Bill was withdrawn. The decision came after extensive consideration of the proposed framework and the difficulties associated with its implementation. Instead of continuing with the same proposal, the government chose to develop a different approach that was intended to provide a more focused framework for digital personal data.

This led to the Digital Personal Data Protection Act, 2023. The Act is specifically concerned with digital personal data and establishes responsibilities for entities that process such information. It also provides individuals with certain protections concerning their personal data. Importantly, the law does not treat all uses of personal information as something that should be stopped. Digital businesses and services often need information to function. The main concern is whether that information is being handled according to the legal requirements and whether appropriate responsibility is placed on the organization using it.

The Digital Personal Data Protection Rules of 2025 add practical details to this framework. While the Act establishes the main legal requirements, the Rules help explain how those requirements are to be followed by the relevant authorities. They provide organizations with more specific directions concerning their duties, compliance, and protection of personal information. Their role is important because effective data protection requires not only broad legal principles but also practical procedures.

India’s approach has therefore changed considerably over time. The first stage was mainly concerned with making electronic activities legally recognized and dealing with cyber-related problems. Later, the focus shifted to the privacy of individuals and the responsible use of personal information. The Srikrishna Committee helped bring these issues to the center of legal discussions. The 2019 Bill represented an attempt to create a dedicated data protection law, although it was eventually withdrawn. The Digital Personal Data Protection Act, 2023, and the Rules of 2025 have now become the basis of the newer framework.

The important point is that data protection is not only about keeping information a secret. It is also about giving people confidence that their information will be handled responsibly. Simultaneously, businesses and public authorities require access to data for legitimate purposes. India's continuing challenge is to protect individuals without preventing the useful development of digital services and technologies.

Definition of Personal Data

The **Digital Personal Data Protection (DPDP) Act, 2023** uses the term personal data for information that is connected to a particular individual and can be used to identify that person. In other words, if information can tell us who a person is, either on its own or when considered along with other information, it can be treated as personal data under the Act. However, information that has been anonymized so that a person can no longer be identified is generally outside the scope of personal data. The same applies to information that is not connected to an identifiable individual.

Definition of Data Principal

The DPDP Act refers to the person whose personal information is involved as the **"Data Principal."** Simply put, the Data Principal is the individual to whom the personal data belong. This idea is somewhat similar to the term **"data subject"** used in the European Union's GDPR. The Act also makes special arrangements for people who may need someone else to act on their behalf. When personal data belongs to a **child below the age of 18**, the child's parent or legal guardian has a role in matters concerning that data. Similarly, when a person with a disability requires a legal guardian to act on their behalf, the guardian can represent the person regarding their personal data.

The DPDP Act primarily addresses information related to **individual human beings**. Therefore, it focuses on protecting the personal data of natural persons rather than treating information belonging to companies or other organizations as personal data under the Act. The central idea is to protect information that can be linked to a real and identifiable individual.

ISSN: 2582-6433

Existing Legal Framework for Data Protection in India: India's data protection laws have developed with the increase in the use of digital technology. Earlier, there was no single law dealing with personal data; thus, protection depended on different laws and legal rules.

A. Constitutional Protection: The Puttaswamy judgment made privacy an important constitutional right. The Supreme Court recognized it under Article 21, which protects life and personal liberty. This provides people with legal protection over important parts of their private lives. However, privacy can be limited when there is a valid legal reason, and the constitutional requirements are followed.

B. Other Legal Protections

1. **Information Technology Act, 2000:** This law deals with electronic activities and cybercrimes in India. It also provides certain safeguards for sensitive personal information, particularly in Section 43A.
2. **Criminal Law:** The Indian Penal Code, 1860, could apply when misuse of information amounted to a criminal offence. It has now been replaced by the Bharatiya Nyaya Sanhita, 2023.
3. **Intellectual Property Laws:** Copyright law can protect an original database when it meets the requirements of copyright law. This protection relates to the work itself, rather than personal privacy.
4. **CICRA, 2005:** The Credit Information Companies (Regulation) Act, 2005, provides rules for dealing with credit information and related records.
5. **Contracts:** Privacy can also be protected through agreements between parties. Confidentiality clauses and non-disclosure agreements can prevent sensitive information from being shared without permission from the concerned parties.

Principles of Data Protection

Article 5 of the General Data Protection Regulation (GDPR) provides organizations with basic guidelines for dealing with people's personal information. In simple terms, the rules are about being honest with people, collecting only what is needed, keeping information correct, protecting it properly, and taking responsibility for how it is used.

1. Lawfulness, Fairness, and Transparency: An organization should have a proper legal reason for using someone's information. People should also know what is happening to their data. They should be able to understand what information is being collected, why it is needed, and how it may be used.
2. Purpose Limitation: There clear reason for collecting personal information. For

example, information provided to open an account should not automatically be used for an unrelated purpose. Any different use should have a legal basis.

3. Data Minimization: Organizations should not ask for information simply because they can acquire it. They should collect only the details that are useful for a particular purpose. This also helps to reduce unnecessary privacy risks.
4. Accuracy: Personal information should be kept reasonably accurate. If an organization discovers that someone's details are incorrect or outdated, it should take steps to correct them instead of continuing to rely on incorrect information.
5. Storage Limitation: There is no need to keep personal information forever. Once the information has served its purpose and there is no legal reason to retain it, it should be deleted or securely disposed of properly.
6. Integrity and Confidentiality: People expect their personal information to be kept safe. Organizations should therefore implement sensible security measures to protect it from hacking, unauthorized access, accidental loss, misuse, or damage.
7. Accountability: An organization cannot simply say that it follows the GDPR; it should be able to show how it does so. This means having appropriate policies, security measures, and procedures for handling personal information responsibly.

7 DATA PRINCIPAL RIGHTS UNDER THE DPDP ACT

Right to Access: If a retailer asks a customer, “What is your personal information about a customer and how are you using it?” that individual should be able to reply. The business should be able to explain why or where it has obtained the information, how it has been used, to whom it has been shared, and the retention period for which the information will be kept. When a customer asks for it, it is a difficult request for businesses to fulfill since the information is typically dispersed across several resources available to the business, including CRM systems, customer-support platforms, analytics platforms, internal databases, third-party applications, and so on. The purpose of this is to aggregate the information and provide one clear picture to the individual of their data and how it will be managed once it involves the business.

Right to Update: People’s details may change over time. They may have moved to a new address, obtained a new phone number, or noticed that their names or other information were recorded incorrectly. They should be able to inform the company about mistakes and request that they be fixed. Businesses should not only correct information in one place. They should ensure that the new details are updated wherever they are being used, including relevant internal systems and, when necessary, with external vendors or service providers.

Right to Withdraw Consent: Sometimes, we agree to let a company use our information and later decide that we are no longer comfortable with it. People should be able to change their mind and withdraw their consent easily. Sometimes, we agree to let a company use our information and later decide that we are no longer comfortable with it. People should be able to change their minds and easily retract their consent.

Right to Erasure: When a business no longer has a real, articulable need to use a person's personal information, then the person should be given the choice of having it removed. If there is no valid reason or there are legal requirements to do so, then this will be determined accordingly. It is the business's responsibility to monitor the location of personal information and the length of retention time required. They must delete the requested data from their systems upon acceptance of the deletion request, as well as manage copies of data they do not hold (if applicable) with backup or external data managers. The individual should also be told if the request has been acted upon.

Right to Nominate: If a person cannot manage their data rights, they may be delegated to a trusted party. If a claim is made for a record of the nominee and verification of that person, a mechanism should be established to record the nominee and confirm the identity of the nominee when a request is made. The nominee can then deal with this person's requests for information on the data, if required.

Right to Raise a Grievance: There should be a clear pathway for the grieved person to raise a grievance and receive support if they think that their personal information has been used or treated in an inappropriate manner or that their data rights have not been respected. To allow for the submission of a grievance in a very easy way, with clear contact information for the responsible privacy team or DPO. They also need to have a mechanism in place to keep an eye on, handle, and react to complaints within the required timeframe.

Right to Access: Consent Notice in Scheduled Languages: Individuals must be able to comprehend a consent notice in a native language. They may request information on consent in a language of their choice from a list of scheduled Indian languages. Businesses need to have consent notices prepared in a language that is acceptable to them and share the notice in the language that the person chose. This will allow individuals to understand how their personal data will be used before consenting.

DIGITAL ECONOMY.

The digital economy is the economy that relies on digital technology for conducting daily activities. Nowadays, individuals can purchase, pay, communicate, work, learn, and use various services via the Internet. Digital devices are also utilized by companies to interact with customers, manage company operations, store details, and make better decisions. The digital economy has flourished thanks to technologies like the Internet, smartphones, cloud services, artificial intelligence and machine learning, sensors, and blockchain.

In 1995, Don Tapscott coined the term ‘digital economy'. The idea has come a long way from then. The earlier use was predominantly to refer to Internet businesses and Internet services. Now, however, it extends far beyond this to encompass a much broader swath of activities in which digital technologies engage with physical devices, machines, data and people. This change is visible in many areas such as healthcare, banking and finance, agriculture and education as well as manufacturing.

India has also been on a fast track to becoming a digitized economy. Smartphones, online payments, e-commerce, digital banking and other technology services have altered the way people and businesses interact with the economy. A McKinsey report earlier estimated that India's digital economy would bring in job opportunities of the order of 60-65 million by 2025. It also estimated that the contribution of the digital sector will be around $355–435 billion to India's GDP by 2025, as compared to the contribution of about $200 billion in 2018. These are further signs of the growing role of digital technology in providing job creation, enhancing business opportunities, and contributing to India's overall economic growth.

GOVERNMENT PART TO SUPPORT THE DIGITAL ECONOMY.

The Indian government has taken several steps towards digital growth and to make technology more user-friendly. To build Digital India and make technology user-friendly, the Government of India has taken several steps. They have contributed to enhancing connectivity, provided incentives for online services and businesses, and provided more awareness about digital tools.

ISSN: 2582-6433

Digital India: This project was launched in 2015, covering aspects of better Internet connectivity, digital infrastructure, and online government services. It has facilitated the use of technology in many fields, such as the public sector, education, healthcare, and banking. UPI was introduced in 2016 and has made digital payments easier and faster. Individuals can move funds instantly between financial institution accounts using their smartphones, and cashless payments are common today.

PMGDISHA: PMGDISHA is a project initiated in 2017 to improve digital literacy among people, especially in rural areas. It teaches basic skills such as using a smartphone, the Internet, and online payments.

Startup India: It is a program for the promotion of startups, entrepreneurship, and innovation. It has been instrumental in creating a more favorable atmosphere for startups and tech concepts.

National Digital Communication Policy 2018: The policy will focus on efforts towards the extension of broadband connectivity, digital technologies, and connectivity, such as 5G. Improved connectivity enables individuals and businesses to participate in the digital economy.

National Artificial Intelligence Mission: The government's focus on AI initiatives is on research, skill-building, and practical applications. AI can help in various industries, such as agriculture, healthcare, education, and manufacturing, as well as open new avenues for innovation and economic growth.

THE 2025 REPORT ON INDIA’S DIGITAL ECONOMY.

According to the 2025 State of India’s Digital Economy Report by ICRIER and PROSUS, technology is becoming an increasingly important driver of the Indian economy. This report explores how digital services are transforming the way individuals, businesses, and institutions operate and interact. It also focuses on the key aspects of the digital ecosystem, including Internet access, digital infrastructure, technology innovation, cybersecurity, and the adoption of digital tools. It checks these areas through the framework of Connect, Harness, Innovate, Protect, and Sustain.

India’s digital growth is easily observed in everyday life. People usually use smartphones and the Internet for activities such as shopping, banking, sending money, communicating, and accessing different services. The increasing use of these digital facilities has helped India become the third-largest digital economy in the world. Digital technology is also becoming increasingly important for India's future economic growth. The report projected that the digital economy may account for nearly 20% of India's GDP by 2029. As digital activities continue to expand and increase, they may create new business opportunities, support employment, improve services, and encourage innovation. This indicates that technology is expected to become an increasingly important part of India's economy in the coming years.

Even though India has made considerable progress, there is still room for improvement, especially in artificial intelligence. Among 32 countries, India ranks 11th in AI research and 16th in AI infrastructure, indicating that future investment and development are needed in this area. To improve its situation, the country needs to focus more on AI research, modern infrastructure, education, and developing people with the right technical skills.

Another important concern is ensuring that digital technology is accessible and useful to everyone. Simply having access to a smartphone or the interest is not enough; people also need the necessary digital skills, knowledge, and confidence to use online platforms and services effectively. Differences in education, location, income, and access to resources can make digital participation easier for some people than others. India's eighth-place ranking in the Connect, Harness, Innovate, Protect, and Sustain index indicates that more efforts are needed to ensure that digital technology reaches a wider population and is affordable, practical, and accessible nationwide.

IMPACT OF DATA PROTECTION ON THE DIGITAL ECONOMY

Introduction: Today, we share a lot of personal information online without even thinking about it. We use mobile banking, make online payments, shop on websites, use social media, and download apps regularly. Because of this, keeping our information safe has become very important. Data protection means keeping personal information secure and preventing it from being misused or accessed by the wrong people. When people feel that their information is safe, they are more comfortable using online services. This trust also helps digital businesses grow.

Review of Literature: Researchers have increasingly examined how privacy, data security, and digital business are connected. Existing studies suggest that protecting personal information is important not only for safeguarding individual rights but also for helping people feel comfortable when using online services. Baxi (2018) discusses the significance of privacy following the Puttaswamy judgment and connects it with trust in digital platforms. Abraham and Hickok (2019) examine the challenge of enabling companies to use data for innovation while respecting people's privacy. Chander and Le (2020) compare India's proposed data protection system with the GDPR and point out concerns about consent and the ability of regulators to enforce privacy rules. Research on digital finance also shows that online services can make transactions easier and more accessible. However, without proper safeguards, users may face privacy and security risks. Schwartz and Peifer (2017) emphasise that well-defined data protection rules can benefit both businesses and consumers by creating clearer responsibilities and greater trust. Overall, the studies reviewed suggest that responsible data use and effective privacy protection are essential for building public confidence and supporting the sustainable growth of the digital economy.

Methodology: The research is based on a legal and interpretive study of India's approach to protecting personal information in the digital economy. It examines the laws and legal decisions that shape the way personal data is collected, processed, and protected. Particular attention is given to the Digital Personal Data Protection Act, 2023, and relevant Reserve Bank of India (RBI) directions. These materials are used to understand what protections are available to individuals and what obligations are placed on organisations handling personal data. The study also draws on published research and other reliable sources to support the discussion. Academic writings, research studies, expert analysis, and reports from relevant institutions are considered for this purpose. In addition, India's system is viewed alongside the European Union's GDPR and selected privacy laws in the United States. This comparison helps place India's legal framework in a wider context and shows how different countries approach privacy, data use, and regulation in the digital age.

Privacy and Its Status as a Fundamental Right: The 2017 Puttaswamy judgment by the Supreme Court marked a significant step in strengthening privacy rights in India. The Court affirmed that individuals have the right to make personal choices and to keep aspects of their lives confidential. This has become increasingly important in the present digital environment, where everyday activities rely heavily on online services. People frequently share their information with banks, websites, mobile applications, and other digital platforms as part of routine use. However, they are not always fully aware of how their data is processed or used after it is provided. For this reason, individuals should be clearly informed about the handling of their personal information and should have real control over how it is collected, stored, and used.

E-Commerce, Consumer Profiling and Data Governance: The rapid expansion of digital shopping in India has significantly transformed consumer behaviour. As online platforms grow, they collect and process vast amounts of user data, including browsing patterns, purchase history, and search activity. This information allows companies to predict consumer preferences and improve service delivery. While such developments enhance convenience, they also raise serious concerns about the extent to which personal data should be used for commercial gain. The DPDP Act seeks to regulate this space, though several practical challenges remain.

- ***i.*** *Influence of Digital Platforms on Consumer Choices: Online marketplaces do not present products neutrally or randomly. Instead, what a user sees is often shaped by their past interactions on the platform. This creates a tailored shopping experience that can feel helpful and relevant. However, it may also subtly guide purchasing decisions. Since users are rarely aware of the logic behind these recommendations, it becomes difficult to determine whether their choices are truly independent or shaped by algorithmic influence.*
- ***ii.*** *Risks Associated with Data Breaches: The storage of large volumes of personal data makes e-commerce platforms attractive targets for cyberattacks. Incidents such as the Juspay breach in 2020 and the BigBasket data exposure in 2021 highlight the vulnerability of digital systems. Beyond immediate privacy violations, such events can significantly damage public trust in online services. This underscores the need for strong cybersecurity measures along with effective regulatory enforcement.*
- ***iii.*** *Limitations of Informed Consent: In most digital platforms, users are required to agree to privacy policies before accessing services. However, these policies are often lengthy, complex, and difficult for the average user to fully understand. As a result, individuals frequently provide consent without being aware of how extensively their data may be collected or processed. This creates a gap between formal consent and genuine understanding.*
- ***iv.*** *Defining Necessary Data Collection: While businesses require certain user information to operate effectively, excessive data collection can lead to privacy concerns. The DPDP Act, particularly under Section 8, emphasises the principle of*

collecting only what is necessary. However, determining what qualifies as "necessary" is not always straightforward. If companies are allowed broad discretion in this interpretation, there is a risk of over-collection of personal data beyond what users would reasonably expect.

v. *Challenges in Exercising Consumer Rights: Although legal frameworks provide mechanisms for grievance redressal, consumers may still face practical difficulties when attempting to assert their rights. Large corporations often have greater technical expertise and legal resources compared to individual users. This imbalance can discourage consumers from pursuing complaints. A more accessible and user-friendly grievance system would strengthen the effectiveness of data protection laws.*

vi. *Comparison with the GDPR Framework: The European Union's GDPR is widely regarded as a comprehensive data protection regime. It includes detailed rules on profiling and automated decision-making, along with stronger safeguards in certain situations. While India's DPDP Act marks an important step forward in regulating personal data, it does not fully replicate the GDPR's approach, especially in relation to algorithmic decision-making and profiling protections.*

vii. *Importance of Consumer Trust: Trust plays a central role in the success of digital commerce. Users are more likely to engage with online platforms when they believe their personal information is handled responsibly. Repeated data breaches or unclear data practices can weaken this trust and discourage participation in digital services. Therefore, safeguarding privacy is essential not only for legal compliance but also for sustaining the growth of the e-commerce ecosystem.*

CHALLENGES OF PROTECTING PERSONAL DATA IN THE DIGITAL ECONOMY

Introduction: Digital technology and internet services have become deeply integrated into everyday life, supporting how people communicate, study, work, shop, and access essential services. Although these tools offer great convenience, they also raise growing concerns about the safety of personal information. Each time individuals use online platforms such as websites, social media, mobile applications, or digital services, they unintentionally generate data about themselves. In many cases, users are not fully aware of what information is being collected, who has access to it, or how long it will remain stored. Once shared online, personal data is also difficult to fully remove, even if a person later wishes to withdraw it or change their views.

In addition, different pieces of information can be combined to build detailed profiles of a person's behaviour, preferences, and lifestyle. If such data is misused or accessed without permission, it can result in serious problems such as fraud, identity theft, surveillance, discrimination, or damage to reputation. This highlights that privacy is not only a technical issue but also a matter of personal rights, trust, and individual freedom. Therefore, safeguarding personal data requires responsible practices from organisations, strong legal frameworks, secure technologies, and greater awareness among users. This paper explores the key challenges involved in protecting personal data and privacy in the digital economy and explains why these issues are becoming increasingly important in today's digital world.

Compliance Complexity: Small and medium-sized businesses may find it challenging to comply with the DPDPA due to its seeming complexity and time-consuming nature. Businesses are often small and lack legal or privacy experts, as well as sufficient staff and budgets. Due to these constraints, they might find it difficult to understand what is required of them and how to implement it in their everyday work. This can lead to inadvertent errors and problems in maintaining good data protection procedures.

The barriers to accessing technology and infrastructure.Issues of technology and infrastructure gaps: For some organisations, data protection may be more challenging because of a lack of appropriate technology. Older computer systems or manual systems can pose difficulties for businesses when it comes to maintaining a secure and organized personal information system. Transitioning to a better system can also be expensive, training and technical support resources can be significant. For smaller businesses that have a limited financial and technical capacity, these problems can be especially heavy.

Striking the Right Balance between Innovation and Privacy: With the continued advancement of technology, companies are discovering new ways to leverage information in their daily operations. But it's important to use data wisely and ensure the safety of individual information. Companies may also be concerned that privacy policies may restrict their ability to experiment with new concepts or implement innovative technology. This is particularly important when dealing with systems that rely heavily on personal data. Businesses must, therefore, be mindful of data usage and retain sufficient flexibility to keep up with the latest technologies and enhance their offerings.

ISSN: 2582-6433

The absence of technology and infrastructure gaps. Lack of technology and infrastructure gaps: It's hard to address data-protection requirements when the organization's technological infrastructure is outdated or not up to the job. Some businesses may rely on outdated programs, unsupported devices, or manual record systems that make it more difficult to maintain personal information security. The upgrade of their digital infrastructure can be a costly and time-consuming process, and extra measures may be required to provide new training. In smaller companies, it might be more apparent because the budgets and technical support might be smaller, making it more difficult to improve data security.

Ambiguity in Regulatory Guidelines: Businesses may sometimes struggle to understand how the DPDPA fits into their particular work practices. Certain situations may leave them unsure about what steps they should take when collecting, using, or managing personal information. If the available guidance does not answer these questions clearly, different organizations may respond to similar situations in different ways. This can make compliance less predictable and create additional difficulties for businesses trying to meet their responsibilities.

Digital Divide: India's digital growth has not reached every community equally. People in rural and remote areas may still experience unreliable internet connections, limited access to smartphones or computers, and fewer opportunities to develop digital skills. These difficulties can affect how easily they access education, jobs, financial services, healthcare, and public services. Without better and more affordable digital access, people in less-connected areas may continue to face disadvantages compared with those living in well-connected communities.

Cybercrime: As more activities move online, protecting people from digital crime has become increasingly important. Criminals may use deceptive techniques to obtain passwords, personal details, or financial information from unsuspecting users. A successful attack can cause financial harm and may also expose sensitive information. Individuals and organizations can reduce these risks by using secure systems, staying alert to suspicious activity, and keeping themselves informed about common forms of online crime.

COMPARATIVE ANALYSIS: The DPDP Act and the GDPR were created to address concerns about the use and protection of personal information. Both frameworks expect organizations to handle data responsibly and take steps to protect individuals' information. However, they differ in how they define responsibilities and provide privacy protections. The

GDPR gives individuals considerable control over their personal data and sets out detailed requirements for organizations. The DPDP Act follows a framework designed for the Indian context, with its own rules governing the collection, use, and protection of personal data.

Consequently, the two laws have a similar purpose but use different legal approaches to achieve it. As digital technology becomes more deeply connected to everyday life in India, protecting personal information has become a growing priority. The DPDP Act sets out responsibilities for organizations when they collect or use personal data and encourages them to handle that information carefully. It also tries to avoid making legitimate business and government activities unnecessarily difficult. However, questions remain about issues such as government exemptions, the rights available to individuals, and the strength of regulatory supervision. Despite these concerns, the Act provides India with a dedicated legal foundation for improving privacy practices and making organizations more responsible for the data they handle.

The DPDP Act sets rules for the handling of personal information in digital form. It covers data that is created or collected electronically, as well as information that is converted from physical records into digital files. The law can also apply to organizations located outside India when their activities involve providing goods or services to people in India.

The main objective of the Act is to improve the protection of personal information and encourage organizations to treat such data responsibly. It places responsibilities on entities that collect or use personal data and provides individuals with certain protections. However, the law does not cover every form of data use. Activities carried out strictly for personal or household purposes are generally excluded, while certain government activities may qualify for exemptions under the Act.

The DPDP Act, 2023, and the GDPR both seek to address growing concerns about the use of personal information online. While they share the broader aim of protecting privacy, their legal approaches are different. The GDPR gives individuals substantial control over their personal data and places detailed obligations on organizations.

The DPDP Act has been structured around India’s own legal and digital needs, with provisions that take into account the activities of businesses and government bodies. For India, the DPDP Act represents an important move toward a more organized system of data protection. It gives organizations clearer expectations for handling personal information and provides a legal foundation for improving privacy practices. Its effectiveness will ultimately depend on how the rules are applied, how well organizations comply with them, and whether the framework can keep pace with technological changes and new uses of personal data.

ISSN: 2582-6433

CONCLUSION

The amount of personal information available online has increased greatly as digital services have become part of everyday life. People regularly leave information behind through social media, emails, websites, applications, and online accounts. Once this information is stored or shared, it may remain accessible for a long time. This can create problems when old information no longer reflects a person's current life, beliefs, or circumstances.

Dealing with these privacy concerns requires more than simply creating laws. Organizations need to collect information responsibly, protect the data they hold, and avoid unnecessary retention. Governments need to provide effective legal safeguards, while individuals should understand the possible risks before sharing sensitive details online. Strong technical security can provide another layer of protection against unauthorized access and misuse.

A person's past should not necessarily become a permanent digital identity. People change as they gain new experiences and their circumstances develop. Privacy practices should therefore provide individuals with meaningful control over their information while still allowing technology to be used for communication, education, research, and innovation. Finding this balance is essential for creating a digital environment that is both useful and respectful of personal privacy.

The DPDP Act, 2023 responds to the increasing need to protect personal information in a world where digital services are widely used. Their purpose is broadly similar, but the way they regulate data is different. The GDPR gives individuals a strong set of protections and requires organizations to meet detailed privacy obligations. The DPDP Act establishes a framework suited to India's own legal and economic circumstances and sets responsibilities for organizations that deal with personal information.

For India, the DPDP Act provides an important foundation for improving data privacy and encouraging safer handling of personal information. Its practical value will depend on how clearly its requirements are understood, how consistently organizations follow them, and how effectively compliance is monitored. The framework may also need to develop over time as technologies such as artificial intelligence, connected devices, and large-scale data systems create new privacy concerns.

ISSN: 2582-6433

Reference:

- researchgate.net
- oecd.org
- ijlmh.com
- aimspress.com
- scribd.com
- asparev.org
- eprajournals.com
- consent.in
- ijraset.com
- vajiramandravi.com
- icrier.org
- uniconsent.com
- atlanticcouncil.org
- policyaccelerator.uncdf.org
- dsci.in
- kpmg.com
- slideshare.net
- visionias.in
- lawyersclubindia.com
- ijapt.org
- blog.ipleaders.in
- atlassystems.com