



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

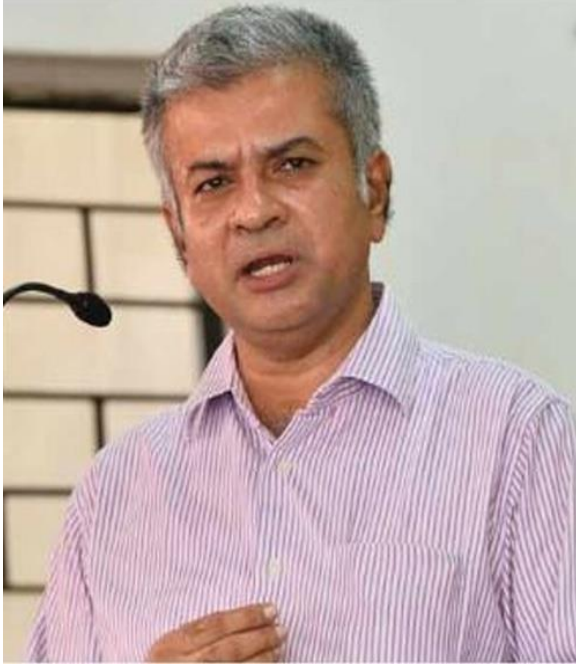
No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

– The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

W H I T E B L A C K
L E G A L

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a

professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat



Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.



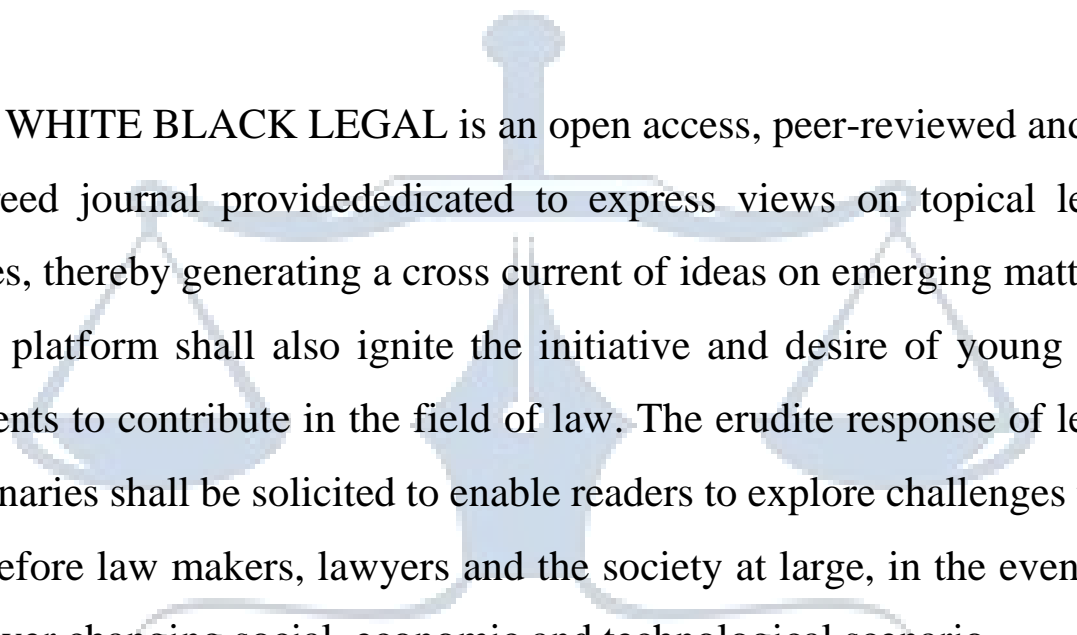
Subhrajit Chanda



BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

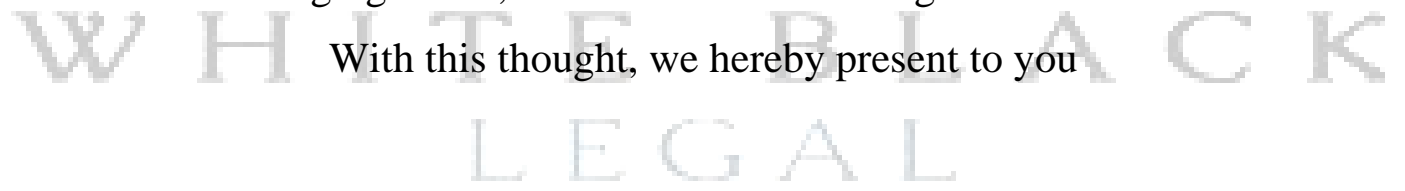
Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you



SECURING THE DIGITAL SELF: EXPLORING THE LEGAL FRAMEWORK AND PRACTICAL IMPLICATIONS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - MS. SHAMBHAVI JAISWAL
STUDENT OF AMITY LAW SCHOOL,
AMITY UNIVERSITY NOIDA
LLB-2021-24

ABSTRACT

Clive Humby at a conference on Association of National Advertisers stated that :

“Data is the new oil. Like oil, data is valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc. to create a valuable entity that drives profitable activity. so, must data be broken down, analysed for it to have value.”¹

This means that data is an important asset that entrepreneurs are exploring to generate significant profits. Consequently, it also emphasises that it is not a waste and can become a useful asset and a tool. We are now also in a very digital economy, where everyone depends on data. Data is better than opinion. It is better because it is more efficient as it can predict results, gain insight into best practices for business, and create better strategies based on the current data which is useful if up-scaling, revenue generation ,etc. by the businesses. However, if data is not managed and handled carefully, it can also cause significant damage and harm. Data is powerful on its own, but the law must help manage and regulate it. Accordingly, data protection and privacy laws were framed and India passed a long awaited law in this regard known as the Digital Personal Data Protection Act, 2023 .

The Digital Personal Data Protection Act of 2023 (DPDPA) and the Information Technology Act of 2000 (IT Act) are the subject of a comprehensive analysis in this research paper. These legislative

¹ <https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/?sh=12843380c208>

frameworks have evolved to reflect the increasing significance of digital technologies and the requirement for vigorous safeguards for personal data in the current era. The DPDPA's advancements to address contemporary digital landscape challenges are highlighted in this paper, which examines the enforcement mechanisms and penalties stipulated by both acts.

In this article, we will discuss everything related to data privacy laws and data protection laws in India.

INTRODUCTION

Humanity is in the midst of a massive technological revolution. Technology is developing rapidly, and it in turn is shaping and becoming more and more ingrained in our own lives, history and future. Recent advances in areas such as information and telecommunications technology are changing lives by providing new ways to exchange information, do business and influence economic and social clusters of societies around the world. These revolutions are very distinct from earlier technological revolutions from the point of view of the speed of development, the relationship between individuals and societies, and the extent of the impact on society. Information technology and its uses have emerged and expanded in a relatively short time. It brought components of business, management and society into one connected and integrated ecosystem. In addition to it, it has completely reformed business practices, administrative structures and cultural interactions.

The Lok Sabha approved the Digital Personal Data Protection Bill on August 7 and the Rajya Sabha approved it on August 9. On August 11, 2023, President Draupadi Murmu approved the Digital Personal Data Protection Bill. This gave India explicit regulation that tends to the insurance of a resident's information. The government will begin the DPDP Law rulemaking process now that the law has been enacted. Businesses and organizations both within India and outside of India could be significantly impacted by this Act. Businesses must abide by stringent compliance requirements in the Act, and failing to do so could result in fines of up to Rs. 250 crore rupees. The information revolution created this infinite spectrum of possibilities. It created a period of rapid invention. While it did increase living conditions, it also showed the limits of government ruling while running for new ways of efficiency, allowing governments to provide investment more effectively. This confrontation could be seen most slit in rule-making. The technological world's legal systems and the society and businesses of today are diametrically different.

Laws and regulations are designed to be stable and long-lasting, while today's technological global environment is constantly in a state of flux. This dichotomy manifests itself in many areas and it adds to the uncertainty caused by the technological revolution and advancement. The disruptive nature of the current technological revolution has made an already uncertain future more difficult to foresee and predict. For example, electronic commerce enabled by information technology is predicted to be the future of world trade, but the form of this trade and its impact on work structure, poverty, standard of living, industry, etc. are still unclear. Another major challenge is that technology can increase inequality around the world. One of the great challenges of the 21st century is to see that it is implemented fairly and equitably despite the effects of electronic commerce.

CHAPTER 1

Data Protection and Data Privacy

DATA AND ITS MEANING

“Section III Privacy & Security states that, data protection requires a holistic approach to system design that incorporates a combination of legal, administrative, and technical safeguards.”²

Personal data is defined under Article 4 sub-clause (1) of GDPR guidelines as:

“ ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”³

Despite the fact that data security and privacy are two distinct concepts with distinct scope and meanings, but they are frequently used interchangeably. Whereas data Privacy only covers personal information; data protection encompasses all types of data, such as personal information. Data privacy can be safeguarded through data protection. The expansion of e-commerce is fundamentally dependent on these two ideas. A reliable, secure, and safe place A reliable communication and information system is essential for gaining the confidence of customers. Personal data security has ethical ramifications. A lot of people argue that people should choose whether to share it, and they

²ID4D guide by World bank <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>

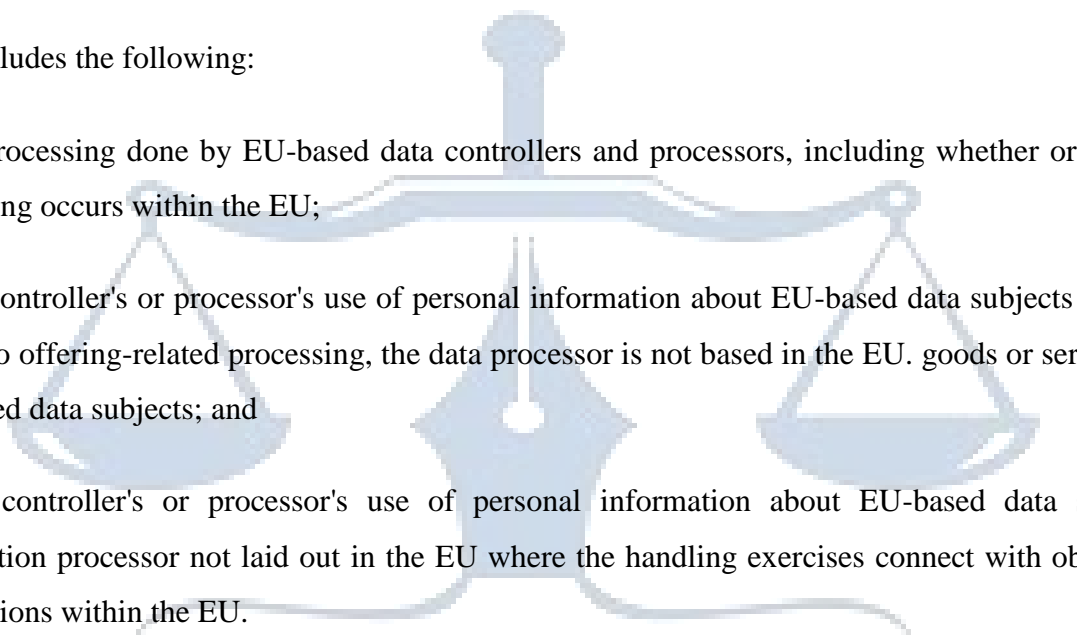
³ https://gdpr-text.com/read/article-4/#comment_gdpr-a-004_1-01

ought to be able to do so in the manner that best suits them. Businesses, customers, and The government recognizes the value of data security, but their approaches differ.

European Union (EU)

The EU has extensive laws protecting personal data. Its laws on data protection are rooted in accordance with Article 8 of the EU Convention and the fundamental right to privacy Sanction on Principal Rights. The General Data Protection Regulation (GDPR) has been drafted by the EU and will go into effect. in May 2018 and will take the place of the 1995 Data Protection Directive.

This includes the following:

- 
- a. the processing done by EU-based data controllers and processors, including whether or not the processing occurs within the EU;
 - b. the controller's or processor's use of personal information about EU-based data subjects when it comes to offering-related processing, the data processor is not based in the EU. goods or services to EU-based data subjects; and
 - c. the controller's or processor's use of personal information about EU-based data subjects information processor not laid out in the EU where the handling exercises connect with observing their actions within the EU.

Additionally, businesses are required to provide an audit trail of consent, which may include screen captures or saved consent documents

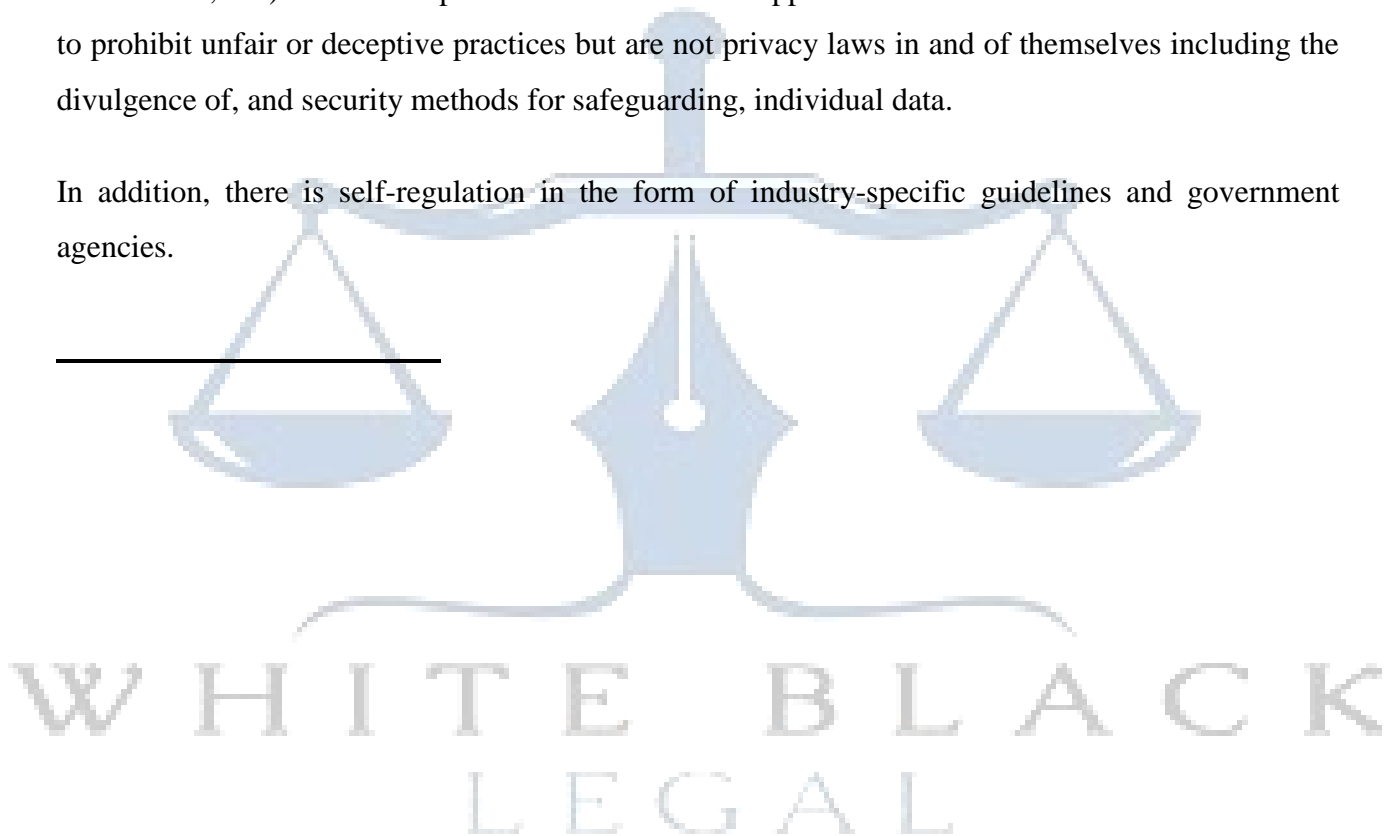
Secondly, the GDPR strengthens the right to be forgotten even more. It states that people have the right to withhold consent, and if they do so, all information about that person to be permanently deleted.

The GDPR framework as a whole is more expansive and much more stringent. punishments for people who don't follow the new rules about how to store and handle personal info. Through adequacy decisions, the EU also exports its rules to other jurisdictions. European The Commission looks at the

laws of a third country and lets data go there if it finds data. protection sufficient in accordance with EU law.⁴

It has so far recognized 11 nations, including the United States In contrast to the EU, the US does not have a single, all-encompassing data protection law. The United States has Personal data collection and use are governed by federal and state regulations. The entire The framework is made up of laws that target particular activities or sectors (such as finance and health ,telemarketing, e-mail for business, etc.) . Consumer protection lends further support to these laws- laws that have been used to prohibit unfair or deceptive practices but are not privacy laws in and of themselves including the divulgence of, and security methods for safeguarding, individual data.

In addition, there is self-regulation in the form of industry-specific guidelines and government agencies.



⁴ European Commission, Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries, Available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed on 5 October, 2017).

CHAPTER 2

Relationship of Law and Technology

Currently, there is no niche that has not been affected by the emergence of technology. Advances in technology have revolutionized every industry. The relationship between law and technology is complex and multifaceted. At the emergent level, technology is the application of knowledge and resources to solve problems or create new products and services. Law, on the other hand, is a set of rules that govern the behaviour of individuals and organizations in society. The relationship between law and technology is constantly evolving as new technologies emerge and new legal challenges arise. For example, the development of the Internet has raised a number of legal issues regarding privacy, intellectual property rights, and electronic commerce. Also, the growth of artificial intelligence has raised concerns about the possibility of job displacement and the need for new laws for the development and use of artificial intelligence. Despite the complexity of the relationship between law and technology, there are several basic principles that can guide our thinking on this issue.

1. First, it is important to understand that law and technology are interdependent. Technology can shape law and law can shape technology.
2. Second, it is important to be aware of the potential conflict between law and technology. As new technologies emerge, it is possible that they will challenge existing laws or create new legal loopholes.
3. Finally, it is important to be proactive in addressing legal challenges created by new technologies. By working together, legal and technology professionals can help ensure that the benefits of new technologies are realized and the risks are minimized.

The use of new technology in law firms is similar to other businesses. New technologies, processes and automation have brought exciting changes and benefits to consumers and businesses. But they also led to the emergence of a new work structure known as the gig economy.

The middle economy is characterized by fixed-term jobs, freelance work and short-

term employment relationships. Proponents of the gig economy argue that it offers unlimited innovation and empowers both workers and entrepreneurs.

Critics, on the other hand, argue that it disenfranchises the workforce and weakens workers' rights. New technologies present both opportunities and challenges. On the other hand, they can be used to automate processes, connect needs to solutions faster and provide companies with a wider supply of employees. On the other hand, they can lead to massive disruptions and loss of individual rights if not carefully considered. It is important to carefully consider the potential impact of new technologies on the workforce and individual rights. We must ensure that these technologies are used in ways that benefit everyone and not just businesses. The IT Act, which was passed at the beginning of the 21st century, set the stage for regulating electronic transactions, as well as stopping cybercrime in India. With advancements in technology and rising concerns The Data Privacy and Protection Act (DPDPA) was enacted in 2023 to establish a more nuanced and comprehensive legal framework for the protection of personal data.

Under the Information Technology Act of 2000, penalties include: The IT Act grants authorities the authority to take severe measures against various cybercrimes. Penalties within Unauthorized access, data theft, and are just a few of the crimes that fall under this category. Hacking. Fines are imposed under Section 43 of the IT Act for system interference, unauthorized access, and introducing malware to computers. Hacking offenses are punishable by imprisonment under Section 66. Moreover, Section 72A addresses the break of privacy and forces punishments for uncovering personal data without permission. Despite its importance during its time, the IT Act has been criticized for not addressing the complexities of current data protection concerns in an adequate manner.

Act to Protect Digital Personal Data in 2023: The DPDPA introduces a more comprehensive and nuanced legal framework in recognition of the need for tighter penalties for violating the privacy of personal data. The Act boldly moves in the direction of international standards for data protection, like the General Data Protection Regulation (GDPR) Union of Europe Penalties for unauthorized processing, storage, or transfer of personal data are outlined in the DPDPA is substantially elevated. Data protection principles are found to have been broken by entities, and as a result, significant fines, ranging from a fixed amount to a percentage of their annual revenue. Repeat offenders face even more severe penalties, including the cessation of activities related to data processing.

Analysis: The approaches to penalties taken by the two acts are a significant distinction. While the IT Act uses a risk-based approach and focuses primarily on fines and jail time for specific offenses, the nature, gravity, and length of the violation are all taken into account by the DPDPA- granting regulatory authorities the authority to tailor penalties in accordance with the particular circumstances of each case.

In addition, the Data Protection Officer (DPO) concept is introduced by the DPDPA, ensuring that organizations adhere to regulations. Refusal to appoint a DPO or follow their instructions results in more punishments. Data is given top priority by organizations thanks to this proactive approach, as an essential component of their operations. 5. **Conclusion:**

The legal frameworks governing its use and protection must evolve with technology, individual freedom. With its pioneering efforts, the IT Act established the foundation for combating cybercrime in India. However, the DPDPA is a significant advancement in recognizing the changing landscape of digital data and the need for regulation that is more sophisticated. The DPDPA's penalties demonstrate a paradigm shift toward a compliance-focused, risk-based approach, bringing India's data protection laws into line with international norms. While the IT Act was useful in, it is time for the DPDPA to emerge as a more robust and adaptable legal instrument that is ready to address challenges that the digital age presents.

The IT Act, which was passed at the beginning of the 21st century, set the stage for regulating electronic transactions, as well as stopping cybercrime in India. With advancements in technology and rising concerns, The Data Privacy and Protection Act (DPDPA) was enacted in 2023 to establish a more nuanced and comprehensive legal framework for the protection of personal data. 2. Under the Information Technology Act of 2000, penalties include: The IT Act grants authorities the authority to take severe measures against various cybercrimes. Penalties within Unauthorized access, data theft, and are just a few of the crimes that fall under this category. Hacking. Fines are imposed under Section 43 of the IT Act for system interference, unauthorized access, and introducing malware to computers. Hacking offenses are punishable by imprisonment under Section 66. Moreover, Section 72A addresses the breach of privacy and forces punishments for uncovering personal data without permission. Despite its importance during its time, the IT Act has been criticized for not addressing the complexities of current data protection concerns in an adequate manner.



WHITE BLACK
LEGAL

CHAPTER 3

COMPLIANCES UNDER THE DPDP ACT

The suitability of the DPDP Act for use

It will be necessary, before delving too deeply into the complexities of the DPDP Act, to first decide if the Act applies and if your business will be subject to the new Act. Such processing on Indian soil is subject to the Act. The Act defines "Personal Data" as any information that can be used to identify a particular individual. The DPDP Act will apply to the processing of such personal data on Indian soil, just as the old bill's draft will.

However, it will be vital to highlight that the Personal Data needs to either have been collected digitally or later digitized, if not collected digitally. It is, therefore, only such digitally kept Personal Data that will be subject to the Act. The Act will apply to the processing of Personal Data regardless of location of the processing, if such processing reflects any activity providing goods or services to the Data Principals within the territory of India. That is even applicable out of the territory.

The Reasons for Processing of Personal Information

The processing of Personal Data on the basis of the Data Principal's Grounds of Consent and Deemed Consent is recognized in Sections 5 and 6 of the DPDP Act 2023, provided that such processing is in accordance with the legal purposes of the Bill.

The Act defines "Personal Data" as any information that can be used to identify a specific individual. The DPDP Act will apply to the processing of personal data on Indian soil, just like the previous bill's draft.

Nevertheless, it is essential to emphasize that the Personal Data must either be collected digitally or subsequently digitized if collected non-digitally. As a result, only digitally stored personal data will be subject to the Act. The Act can apply to the processing of Personal Data regardless of the location of the processing, as long as the processing relates to any activity offering goods or services to Data Principals within the territory of India. This applicability even extends beyond extra-territorially. This Act is very broad in scope and has the potential to affect a number of Indian businesses. As a result, businesses must be aware of the bill's compliance requirements more and more.

Obligations for Consent and Notification

The primary rationale for processing PD remains consent. The DPDP Act, 2023 imposed a very high bar for consent. To be more precise, it has to be voluntary, specific, informed, unequivocal, and unambiguous expression of the wishes of the data principal, given by means of a distinct affirmative action.

The following are examples of consents:

1. Each assent solicitation should be accompanied by a notice from an information guardian. A notice should have data about how an information chief might practice their right to withdraw consent and how they can exercise their right to grievance redress as required by the, file a complaint with the Data Protection Board (the "Board").
2. Administration centrale.- The requirement to give consent is made compulsory by the DPDP Act 2023. Such additional information and the formats prescribed by the government for such notices. As soon as "reasonably practicable," such a similar notice should be given for processing PD for which consent was taken before the passage of the DPDP Act 2023 effect.
3. There is no lookback period for this exercise in the statute. However, Act 2023 elaborates that data fiduciaries may process PD until principal data withdraws consent. Whenever consent is solicited, a notice should be given, and a new notice should be given where prior consent has been sought for processing. Letting these in notification to be taken through the system of assent managers, which are incorporated in the Act, may help in resolving some of the assent fatigue that might arise from the above-mentioned scenario.
4. Information Trustees can continue handling Information for whose processing assent was taken prior to the Act's enactment through the distribution of notice in the prescribed format, and Businesses will appreciate the Act's clarification that Data Personal data may be processed by fiduciaries until the Data Principal pulls out assent.

Legitimate Uses

The DPDP Act of 2023 revisits the idea of 'deemed consent' introduced by the DPDP Bill of 2022. Under this act, a data fiduciary is allowed to utilize the personal data of an individual without explicit permission for specific "legitimate uses." These include:

1. When someone willingly provides their personal data to a company and hasn't objected to its use.
2. Utilization of personal data for employment purposes or to protect an employer from potential harm or legal issues, such as corporate espionage or protecting intellectual property.
3. Meeting legal obligations to disclose information to the government or its agencies, as defined by the Indian Constitution, while ensuring compliance with other relevant laws.
4. Responding to urgent medical emergencies where there's a risk to life or immediate health.
5. Provide assistance during disasters or times of public unrest to ensure safety and support.
6. Adhering to legal orders or judgments issued by authorities.

In simpler terms, these provisions allow companies and authorities to use personal data in specific situations where it's necessary, either for legal compliance, emergency response, or safeguarding interests.

The DPDP Act 2023 introduces a new provision allowing the Central Government to set time periods for different classes of data custodians to determine when a purpose for processing PD is deemed to be fulfilled.

Additionally, the DPDP Act 2023 mandates PD breach reporting requirements for data custodians. This includes any unauthorized processing or accidental disclosure of PD compromising its confidentiality, integrity, or availability.

Processing Children's Personal Data Under the DPDP Act 2023, -A 'child' is defined as an individual below the age of 18 in India. Before processing personal data belonging to a child or a person with a disability under the care of a legal guardian, data custodians must obtain verifiable parental or guardian consent. This requirement extends to obtaining consent from a disabled person, which is a new provision introduced in the DPDP Act 2023.

Furthermore, data custodians are prohibited from tracking or monitoring children's behavior or targeting them with advertising. They are also barred from processing PD likely to adversely affect a child's well-being.

However, certain classes of data custodians may be exempted from these obligations regarding verifiable consent and tracking/monitoring/targeted advertising, subject to conditions prescribed by the government.

Moreover, the Central Government is empowered to specify the age above which certain data custodians will be exempt from these obligations, provided the processing of children's PD is conducted securely.

Obligations of Significant Data Custodians (SDCs)

Recognized as a special category of data custodian, Significant Data Custodians (SDCs) are designated by the central government based on specific criteria. According to the law, SDCs must conduct periodic audits, data protection impact assessments, and appoint an independent data auditor and a data protection officer. The data protection officer should be based in India and report to the SDC's Board of Directors or relevant governing body. They also serve as the point of contact for the SDC's grievance resolution mechanism.

Data Processor Responsibilities

Unlike the DPDP Bill 2022, the DPDP Act 2023 does not explicitly impose obligations on data processors. However, data custodians are responsible for ensuring compliance with the law, including when a data processor processes data on their behalf. Therefore, data custodians must ensure that data processors cease processing PD upon consent withdrawal, delete PD when processing activities are complete, and safeguard PD under their control. It's likely that data custodians will contractually delegate these responsibilities to data processors.

The State and its instrumentalities enjoy extensive exemptions from DPDP Act 2023 obligations, including a general exemption for reasons such as national security and public order.

Furthermore, the Central Government may exempt certain classes of data custodians, such as startups, from specific provisions of the law. Within five years of the law's enactment, it may notify provisions that will not apply to certain data custodians or classes thereof for a specified period.

Rights of Data Subjects

The DPDP Act 2023 retains key rights for data subjects, such as accessing information about their PD processed by a data custodian, seeking correction or erasure of PD, and availing grievance redressal mechanisms. Some of these rights may be restricted when processing is based on 'legitimate use.'

Consent Managers Introduced in the DPDP Act 2023, consent managers serve as a single point of contact for data subjects to provide, revoke, and administer their consent through an accessible, transparent, and interoperable platform. Consent managers must be registered with the Board and accountable to data subjects. They can also file complaints with the Board on behalf of data subjects and may be investigated by the Board for breaching registration conditions.

Data Protection Board

The Board is responsible for investigating PD violations, imposing penalties for non-compliance, and issuing binding directives for effective law enforcement. However, it lacks the authority to enact subordinate legislation under the DPDP Act 2023.

The DPDP Act 2023 includes a comprehensive appeals mechanism. Dissatisfied parties may appeal Board orders or directions to the Telecom Disputes Settlement and Appellate Tribunal and, if necessary, the Supreme Court within specified time frames.

Authority of the Central Government The Central Government has the power to issue notifications, establish regulations, and request information from the Board or intermediaries under the Information Technology Act of 2000. It can issue blocking orders to prevent data custodians from offering products or services to Indian data subjects upon receiving a Board reference.

Voluntary Commitments & Penalties Under the DPDP Act 2023, individuals subject to Board proceedings for non-compliance may provide voluntary undertakings to rectify violations. Acceptance of a voluntary undertaking precludes further DPDP Act 2023 proceedings regarding its contents. Violations of voluntary agreements are considered breaches of the law.

Non-compliance can lead to civil liability under the DPDP Act 2023, with penalties ranging from INR 10,000 to INR 250 crores. These penalties align with those envisioned by the DPDP Act 2022, with the addition of penalties for breaching Board-accepted voluntary undertakings.

Compliance with the Information Technology Act

Information Technology Act, 2000, and its subsequent amendment in 2008 govern personal data protection in India. Compliance includes appointing a dedicated Data Protection Officer, conducting regular risk assessments, establishing transparent data handling policies, providing employee training, and conducting audits to ensure compliance.

Chapter 4

An Overview of the UK Code of Practice for Cyber Governance

Introduction

In today's digital age, the United Kingdom understands the crucial need for strong cybersecurity to safeguard businesses, individuals, and national interests. To tackle the ever-changing cyber threats, the UK Cyber Governance Code of Practice was introduced to guide organizations in establishing effective cyber governance structures. This document serves as a detailed overview, exploring the key aspects, principles, and impacts of the code.

Background:

The UK Cyber Governance Code of Practice was introduced by the government to bolster organizations' cyber resilience. It was crafted in response to the increasing complexity of cyber threats and the necessity for a unified approach to cybersecurity governance. The code offers guidance to organizations of all sizes, urging them to adopt a proactive and risk-aware approach to cybersecurity. The majority of UK organizations heavily rely on digital technologies for their operations. As the digital landscape expands, so do the risks associated with cybersecurity, posing significant threats to many companies. With increased digitalization comes greater opportunities for malicious actors to exploit vulnerabilities and disrupt business activities. Organizations are now more vulnerable than ever to both intentional and accidental cyber incidents.

This new risk environment is dynamic and moves faster than traditional business risks. Cybersecurity risks are amplified by the rapid pace of digitalization, the growing interconnectedness of digital networks, and evolving threats from both state and non-state actors. This complexity is further compounded by the ever-changing regulatory frameworks, both domestically and internationally.

Key Aspects of the Code:

Leadership and Governance: The foundation of the code lies in promoting strong leadership and governance to manage cyber risks effectively. It encourages organizations to establish clear lines of responsibility for cybersecurity, with board members actively involved in overseeing and understanding the organization's cyber resilience strategy.

Risk Management: Effective risk management is a central theme in the code. Organizations are urged to conduct regular risk assessments to identify potential threats and vulnerabilities. The code stresses the importance of aligning risk management strategies with the organization's overall

business objectives.

Awareness and Training: Acknowledging human error as a significant contributor to cyber incidents, the code emphasizes the need to foster a cybersecurity-aware culture within organizations. This involves providing regular training for employees at all levels to equip them with the skills to identify and respond to cyber threats.

Incident Management: The code emphasizes the importance of having a robust incident management plan in place. This includes clear procedures for reporting and responding to cyber incidents promptly. Establishing communication protocols and learning from incidents are vital aspects of this aspect of the code.

Technical Measures: From firewalls to encryption, the code provides guidance on implementing technical measures to secure systems and data. It encourages organizations to stay updated with technological developments and deploy state-of-the-art security solutions.

Supply Chain Security: Recognizing the interconnected nature of today's business environment, the code highlights the importance of ensuring the cyber resilience of the entire supply chain. Organizations are encouraged to assess and manage the cyber risks associated with their suppliers and partners.

Principles Underlining the Code:

Proportionality: The code advocates for a proportionate approach to cybersecurity, recognizing that the level of risk and appropriate mitigation measures may vary depending on the size and nature of the organization.

Integration with Overall Governance: The principles of the code emphasize integrating cybersecurity governance with overall organizational governance. This ensures that cybersecurity is not treated as a separate function but is embedded in the organization's strategic decision-making processes.

Risk Assessment and Management: A risk-based approach is fundamental to the code. Organizations are expected to assess their specific risks and tailor their cybersecurity measures accordingly. Regular risk assessments and updates to the risk management strategy are encouraged.

Internal and External Communication: Effective communication is highlighted as a key principle. This includes communication within the organization to ensure that all relevant stakeholders are aware of cybersecurity policies and procedures, as well as external communication in the event of cyber incidents.

Continuous Improvement: The code stresses the dynamic nature of the cyber threat landscape. Organizations are encouraged to continuously review and enhance their cybersecurity measures to

adapt to evolving threats and technologies.

Implications for Organizations:

Legal and Regulatory Compliance: Adhering to the code is not only best practice but also carries legal and regulatory implications. Organizations may be required to demonstrate compliance with the code as part of regulatory requirements, and failure to do so could result in legal consequences.

Reputation Management: In an era where data breaches and cyber incidents can severely damage an organization's reputation, following the code helps in building and maintaining trust with customers, partners, and the public. Demonstrating a commitment to robust cybersecurity measures enhances an organization's reputation.

Business Continuity: Implementing the code's principles contributes to enhancing an organization's business continuity. By effectively managing cyber risks, organizations can mitigate the impact of potential cyber incidents, ensuring the continuity of operations.

Competitive Advantage: Organizations that successfully implement the code's recommendations can gain a competitive advantage. As cybersecurity becomes an increasingly important criterion for business partners and customers, organizations with strong cyber governance are likely to be preferred over those with weaker measures.

International Collaboration: Given the global nature of cyber threats, adherence to the UK Cyber Governance Code of Practice positions organizations to collaborate internationally. Common cybersecurity standards and practices facilitate smoother interactions and collaborations with entities from other regions.

International Approaches to Cyber Governance:

Globally, several other countries are prioritizing cyber governance and encouraging greater engagement from directors, such as the US through its SEC rules. Industry associations like the US National Association of Corporate Directors and the Australian Institute of Company Directors have also published key principles to support directors in meeting national regulatory frameworks' requirements. The US National Institute of Standards and Technology recently launched the first draft of its Cyber-security Framework 2.0, emphasizing governance as a crucial aspect.

Conclusion:

The UK Cyber Governance Code of Practice offers a comprehensive and adaptable framework for organizations to enhance their cybersecurity measures. By focusing on key aspects such as leadership, risk management, and technical measures, and adhering to underlying principles like proportionality and continuous improvement, organizations can build a resilient cybersecurity posture. Following the

code goes beyond mere compliance, offering tangible benefits in terms of legal standing, reputation management, and competitive advantage. As the cyber threat landscape continues to evolve, the code remains a crucial tool in strengthening organizations' digital defenses across the United Kingdom.



W H I T E B L A C K
L E G A L

CHAPTER 5

SPDI GUIDELINES AND PRIVACY LAWS

In India, we don't have specific laws solely dedicated to safeguarding data. Instead, the Information Technology (IT) Act of 2000, particularly the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011," governs the privacy and protection of data.

Data is generally categorized into two groups: **Personal Data and Sensitive Personal Data**. According to the IT Act, data encompasses various forms of information or instructions processed in a computer system or network, whether stored internally or externally.

Sensitive personal data includes sensitive information like passwords, financial details, health records, sexual orientation, and biometric data.⁵

Apart from the IT Act, certain provisions in the Indian Constitution safeguard individual rights such as the right to life and personal liberty under Article 21, and freedom of speech and expression under Article 19(1)(a), which implies the right to privacy as a fundamental right.

Data protection is crucial to prevent misuse of information, especially given the abundance of personal data online. Privacy and data protection are closely intertwined, and any unauthorized sharing of personal information violates privacy.

Currently, the Information Technology Act and its 2011 Rules govern privacy and data protection. These rules encompass provisions for compensation for negligence, punishment for unauthorized disclosure, and definitions of personal and sensitive data.

According to the IT Rules 2011, personal information is any data related to a natural person that can identify them, directly or indirectly, while sensitive personal data includes categories like passwords,

⁵ [https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511\(1\).pdf](https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf)

financial details, and health records.

These rules apply to entities in India and establish specific provisions for sensitive personal data protection. While a comprehensive Privacy Bill is pending, these rules provide detailed protection for sensitive personal data.

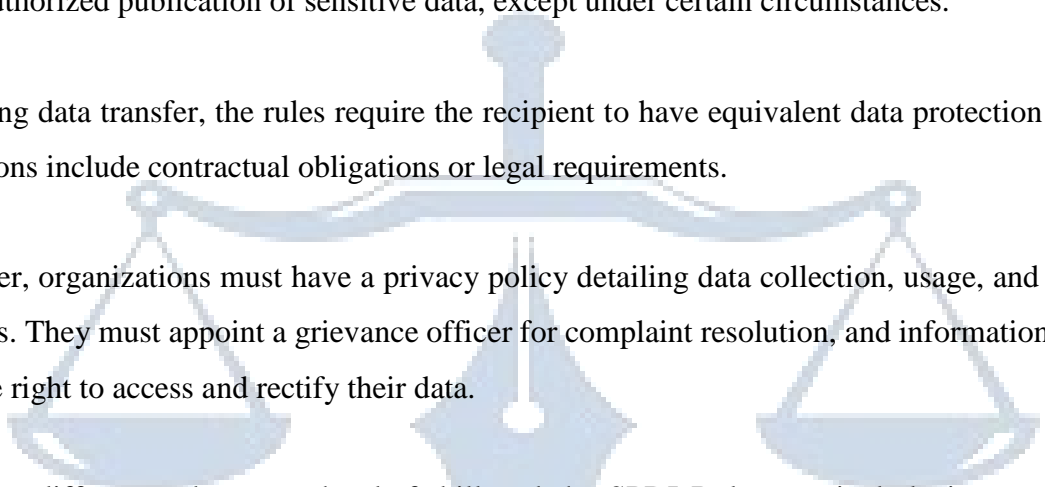
The rules outline rights for information providers, such as the right to consent withdrawal and the right to review and amend data. They also mandate reasonable steps for data protection and prohibit the unauthorized publication of sensitive data, except under certain circumstances.

Regarding data transfer, the rules require the recipient to have equivalent data protection measures. Exceptions include contractual obligations or legal requirements.

Moreover, organizations must have a privacy policy detailing data collection, usage, and disclosure practices. They must appoint a grievance officer for complaint resolution, and information providers have the right to access and rectify their data.

There are differences between the draft bill and the SPDI Rules, particularly in scope, consent mechanisms, data storage requirements, and cross-border data transfer regulations.

Given data privacy's significance as a fundamental human right, stringent laws are necessary to regulate data processing, protect individual rights, enforce access controls, and penalize unauthorized access.



WHITE PAPER
LEGAL

CHAPTER 6

EFFECTIVENESS OF DPDPA IN THE INDIAN LANDSCAPE

The DPDP is a nascent legislation in India with a set of distinct and revolutionising features concerning the right to privacy of each individual. The Act aimed at highlighting the constructive and detailed provisions to secure privacy rights of individuals in India. The key features of the Act are emphasized below for detailed discussion :

1. The DPDP Act has a broad scope, including extraterritorial application for data processing beyond India if it pertains to goods or services within the country.
2. It offers a comprehensive definition of personal data, encompassing any data related to an identifiable individual. Furthermore, the Act expands the scope of the data principal to include parents, lawful guardians of children, and individuals with disabilities.
3. The DPDP Act includes a specific provision for handling the processing of personal data concerning children, stipulating that consent from the lawful guardian is required before doing so.
4. The Data Fiduciary must refrain from any data processing that could harm the well-being of a child. Additionally, they are prohibited from engaging in tracking or behavioral monitoring of data or targeted advertising aimed at children.
5. The DPDP Act provides provisions to accommodate start-ups and grant them an exemption. This approach acknowledges the challenges faced by these start-ups in implementing this dynamic legislation, aiming to foster creativity and innovation.
6. The DPDP Act includes specific provisions outlining the obligations imposed on Data Fiduciaries, such as implementing the provisions of this Act, establishing reasonable security measures to prevent breaches, and providing notice for consent, among others.
7. The DPDP Act bestows upon the Data Principal a range of rights that they can exercise concerning their data. These rights encompass the right to access information, right to rectify data, right to complete data, right to nominate, and right to seek grievance redressal.
8. The Act mandates obtaining consent for processing and collection of personal data. In cases involving the processing of personal data relating to a child, it requires verifiable parental consent. This consent must be freely given, specific, informed, unconditional, and unambiguous. It can also be withdrawn at a later stage. Furthermore, the Act places an obligation on the data fiduciary to furnish a comprehensive notice to the data principal either during or prior to seeking consent.

9. This notice must provide information about the data being collected and the purposes for which it is being collected, as well as a description of individuals' rights and the process for addressing grievances.

10. The DPDP Act has also introduced the role of consent managers. These managers oversee the collection, modification, and revocation of consent, serving as intermediaries in these processes.

11. Under the DPDP Act, a distinction is drawn between a data fiduciary and a significant data fiduciary based on factors such as data volume, sensitivity, risk, and security considerations. Significant Data Fiduciaries are subject to additional obligations, including the appointment of data protection officers, the conduct of data protection impact assessments, and periodic compliance audits.

12. The DPDP Act establishes Data Protection Boards, outlining their formation, member qualifications, remuneration, grounds for disqualification, resignation procedures, and more. Empowered to enact immediate remedial actions in the event of personal data breaches, conduct inquiries, and impose penalties, the Act asserts the board's independence and its function as a digital office.

13. Additionally, the DPDP Act specifies that if a complaint is deemed suitable for mediation, the board is authorized to instruct the involved parties to pursue a mutually agreeable resolution.

Shortcomings and Criticism of DPDP Act

Although the DPDP Act seems to be a good drive towards acknowledging privacy and the freedoms it avails, in reality it has more loopholes than the biggest loophole of its nonexistence. To look at criticism of this righter perspective, the following views with regard to DPDP Act are critical:

1. It applies only to digital data or non-digital data that is subsequently converted into digital but not untransformed data. That is, the law has the following trend application: the law applies to protecting your right to privacy when your data is in the form of digital and does not apply when it is in the form of books and other forms that are offline .

2. It does not provide for both forming categories such as sensitive data, critical personal data e.g ., though stated in its draft stages, being the language used to support the statement in the speech to pass the law, no comprehensive formation is provided.

3. The more serious and private the data are, the stronger it should be. However, it fails to recognise that. The DPDP Act has a lot of exemptions and with numerous exemptions not only limited to start-ups to fasten innovation and growth. But the exemptions are also extended to government and

other government instrumentalities with unrestricted and unchecked power to collect and process data

4. Another criticism about the DPDP Act is it reduces access to information, taking an example of the Right to Information Act ,2000. Under section 8 of the RTI Act, a Schedule allows for 10 exemptions, as per which personal information is exempt from disclosure unless it has no relationship with public activity. However, in the DPDP Act, all personal information is exempt from disclosure. It aimed to strike at foundation of transparency, responsibility and accountability in information technology ecosystem.

5. In reference to the cross border exchanges, the Act states that the Central Government has the control to confine it. Taking after this approach, not sufficient assurance is allowed to the individual information of a person through the Act. Another genuine concern raised within the Act was the issue of the freedom of the Information Security Board.

6. The Act states it to be an autonomous body, but considering the term of the arrangement and the part of the government in its working, it's difficult to acknowledge that the board would be independent.

7. The victory of the DPDP Act depends on people's mindfulness approximately their rights and obligations. They ought to be mindful around the noteworthiness of their individual information, how it is collected and handled and how to redress their grievances as well.

CHAPTER 7

KEY JUDGEMENTS ON PRIVACY LAWS IN INDIA

**JUSTICE K S PUTTASWAMY (RETD.), AND ANR. VERSUS UNION OF INDIA AND ORS.⁶
LAID DOWN THE FUNDAMENTAL OF LAWS OF PRIVACY IN INDIA.**

Understanding the Essence of Privacy: Exploring its Natural Elements

Privacy, often deemed a fundamental right, embodies the essence of personal autonomy and dignity. It stands as a cornerstone of individual liberty and finds resonance in various legal frameworks globally. Rooted in the ethos of liberty and dignity, privacy finds its voice in Article 21 of the Constitution, shaping the narrative of human existence. While it is intrinsic to the jurisprudential fabric, its dimensions extend beyond mere spatial control, encompassing autonomy in judgment and control over personal information.

This right, with its multifaceted nature, transcends definitional boundaries, embodying both normative and descriptive elements. It safeguards physical and mental integrity and assumes paramount importance in the constitutional ethos. Despite its abstract nature, privacy remains a fundamental aspect, intricately woven into the fabric of our rights framework.

Privacy, as enshrined in various articles of Part III, underscores the centrality of individual autonomy. It serves as a bulwark against arbitrary state action, ensuring that citizens remain at the forefront of constitutional discourse. Its significance lies not in rigid definitions but in its dynamic interplay with evolving societal norms.

Recognizing the Inherent Value of Privacy: A Right for All

Privacy, far from being an elitist concept, stands as an inclusive right, accessible to every individual. It underscores the foundational principles of liberty and dignity, weaving a tapestry of rights that safeguard individual autonomy.

As a common law and fundamental right, privacy finds expression in diverse legal contexts. Whether in civil or criminal law, its essence remains unchanged, serving as a shield against unwarranted

⁶ WRIT PETITION (CIVIL) NO. 494 OF 2012- EQUIVALENT CITATION-AIR 2018 SC (SUPP) 1841

intrusion. From property rights to technological advancements, privacy extends its protective mantle over various spheres of life.

Embracing the Nuances: Privacy in the Digital Age

In the digital realm, privacy assumes new dimensions, encompassing informational and technological domains. Concepts like the right to identification and control over personal data underscore the evolving nature of privacy rights. While it safeguards individual autonomy, it also navigates the complexities of a data-driven world, balancing rights with societal interests.

Navigating Limitations: Privacy in the Constitutional Framework

While privacy holds intrinsic value, it is not an absolute right but subject to reasonable restrictions. State interests, ranging from national security to public welfare, justify encroachments on privacy rights. However, such intrusions must meet stringent standards, ensuring a delicate balance between individual liberties and collective interests.

Dignity as the Bedrock: Upholding Fundamental Rights

At the heart of privacy lies the concept of dignity, intertwining with the fabric of fundamental rights. It serves as a beacon of individual autonomy, ensuring that each person can live a life of dignity and freedom. Whether enshrined in Article 14 or echoed in the lamps of freedom under Article 19, dignity remains the cornerstone of constitutional discourse, underscoring the intrinsic value of privacy rights.

CONCLUSIONS

While the DDPA addresses a critical step in the right direction in information security, Obstacles remain. Both implementation and enforcement necessitate sufficient assets, and there are worries about the effect on private ventures. Maintaining a delicate balance between innovation and privacy rights task that necessitates constant dialogue and adaptation. . The DPDP Act, in contrast with the Information Technology Act, 2000, mirrors the developing necessities of a digitized society. By enhancing individual rights, introducing comprehensive provisions, the DDPA establishes the foundation for addressing contemporary issues. framework for data protection that is more resilient and adaptable. As innovation keeps on propelling, a proceeded with obligation to refreshing and refining these legitimate systems will be fundamental to guarantee the successful insurance India's digital data.

The physical and technological components of the Internet, as well as the applications of data generated and transferred over the Internet, as well as the ensuing legal complications. In order to address both the rapid technological change and the resulting inequality, Legal efforts must be made on two levels, as stated in the Introduction.

This control safeguards them from any future rivalry as well. Breaking the despite the fact that a virtuous cycle of data collection may not be practical or desirable, appropriate laws and regulations can ensure that such businesses do not exploit their position in the market and entry barriers for Small and new players are kept to a minimum.

Responsibilities of Data Custodians

As a data custodian, his primary role revolves around ensuring compliance with the law for any processing activities conducted by him or on his behalf by a data processor. Under the DPDP Act 2023, certain erasure requirements are imposed on data custodians. These requirements specify instances where you must delete personal data (PD), such as when it is reasonable to assume that a specific purpose for processing PD is no longer valid.

REFERENCES

1. <https://blog.usecure.io/digital-personal-data-protection-act-of-india-dpdp>
2. [https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511\(1\).pdf](https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf)
3. <https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/?sh=12843380c208>
4. Digital Personal Data Protection Act, 2023 (DPDP)
7. UK CODE ON CYBER GOVERNANCE
8. European Commission, Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries, Available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed on 5 October, 2017).