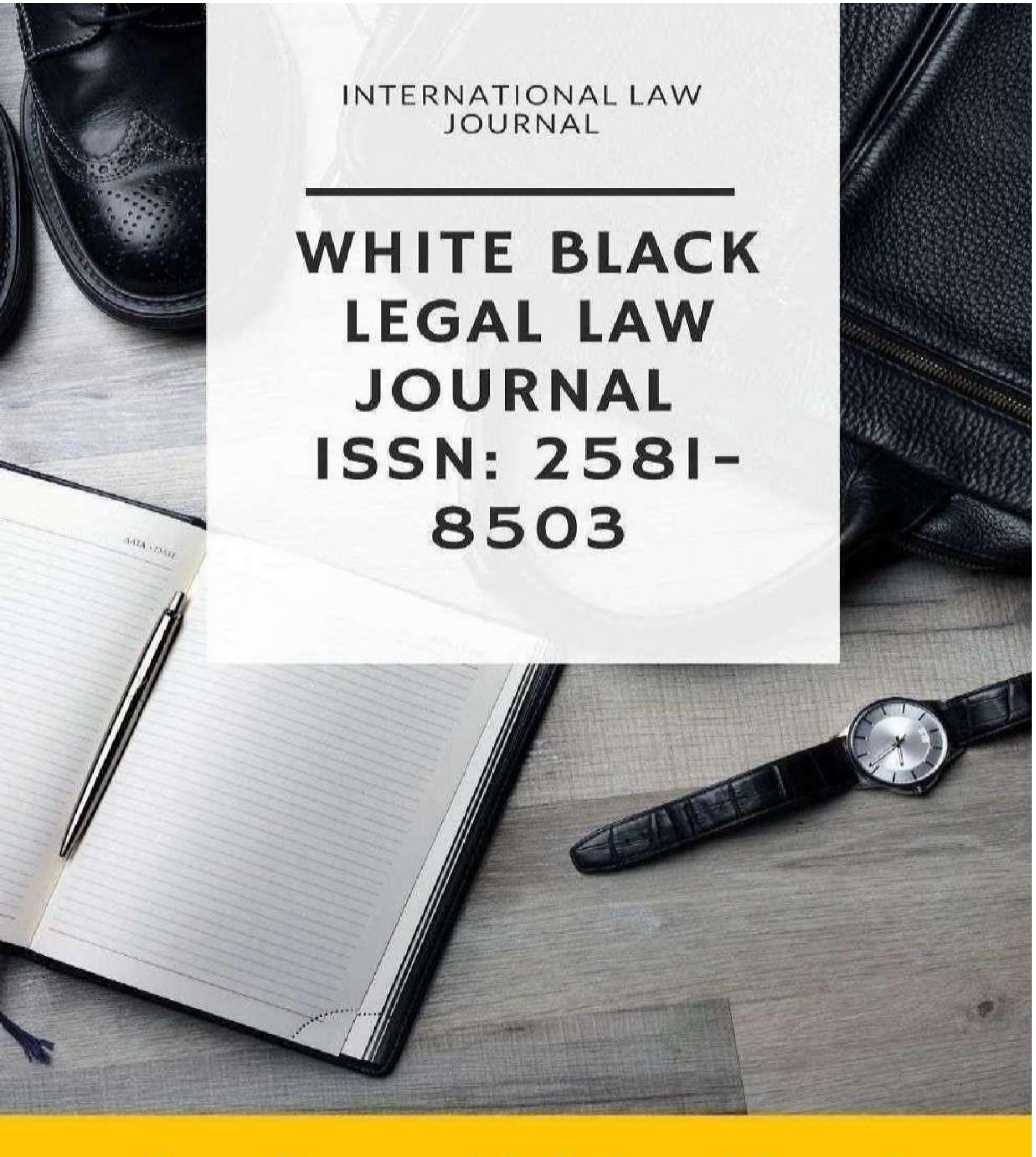

INTERNATIONAL LAW JOURNAL

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.

WHITE BLACK
LEGAL

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 provide dedicated 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

WHITE BLACK
LEGAL

"EVALUATING THE LIMITATIONS OF THE DIGITAL PRIVACY DATA PROTECTION ACT, 2023: A CRITICAL ANALYSIS"

AUTHORED BY - DR.V.PRABHA
Associate professor
Sri Manakula Vinayagar – Centre of Legal Education, Puducherry.

Abstract

The Digital Privacy Data Protection Act, 2023 (DPDPA) was introduced to safeguard individuals' personal information and regulate how organizations process and store such data. However, its effectiveness in achieving these objectives has been widely questioned. This article critically examines the inherent weaknesses in the DPDPA and how these shortcomings have rendered it fruitless in protecting data in the modern digital era.

One major flaw lies in the DPDPA's inability to keep pace with rapidly developing technologies and new data collection practices. With the rise of artificial intelligence, big data analytics, and cloud computing, vast amounts of personal information are being collected, processed, and shared, often without users' unequivocal consent or knowledge. The Act's static dogmatic framework struggles to address such complex and dynamic data flows, leaving individuals vulnerable to privacy breaches.

Another issue is the ambiguity in enforcement mechanisms and accountability measures. Many organizations exploit loopholes in the legislation, leading to minimal compliance or superficial measures that fail to ensure meaningful data protection. Moreover, regulatory bodies often lack the resources or expertise needed to monitor compliance effectively, creating an enforcement gap that diminishes the DPDPA's deterrent effect.

The Act also falls short in educating individuals about their data rights and empowering them to take control over their personal information. Many individuals remain ignorant of how their data is collected and used, disheartenment the DPDPA's aim of fostering clearness and trust.

WHITE BLACK LEGAL

This article highlights case studies where the DPDPA has failed to prevent large-scale data breaches and explores how these failures have eroded public confidence in regulatory frameworks. It concludes by recommending reforms to strengthen the Act, such as adopting more dynamic legislative approaches, enhancing enforcement capabilities, and aligning domestic laws with international standards like the General Data Protection Regulation (GDPR). Without such changes, the DPDPA will continue to fall short of its goal to protect personal data in a digital world.

1. Introduction

Laws related to Data protection become the keystone of the digital era, aiming to protect person’s privacy and guarantee the safe and sound usage of personal information. Amongst these, the Digital Privacy Data Protection Act (DPDPA) has been crucial in various jurisdictions. However, regardless of its well-intentioned goals, there is a growing consensus that the DPDPA has noteworthy precincts and is not as effective as it needs to be in addressing contemporary challenges. This article explores the reasons behind the ineffectiveness of the DPDPA, examining its structural flaws, enforcement issues, and the evolving nature of threats to data security and privacy.

2. Understanding the Digital Privacy Data Protection Act,2023

The Digital Privacy Data Protection Act, 2023 was introduced to provide individuals with control over their personal data, define the farm duties of organizations managing such data, and create a structure for legitimate data dispensation. Its principles classically accentuate intelligibility, justice, answerability, and security. While these are dignified goals, the Act struggles to meet its objectives in practice due to various factors.

3. Structural Weaknesses in the DPDPA

3.1. Outmoded Provisions

Data protection laws often lag behind technological advancements. The rapid pace of innovation, such as the rise of big data, artificial intelligence (AI), and the Internet of Things (IoT), has rendered many provisions of the DPDPA obsolete. For instance:

The definition of personal data may not cover up-and-coming forms of data, such as biometric or behavioral data.

The Act may not adequately address the complexities of algorithmic decision-making and AIdriven profiling.

3.2.Vagueness in Key Terms

The DPDPA repeatedly relies on vague terms like "reasonable measures" or "sufficient safeguards," leaving room for varied interpretations. This ambiguity undermines the consistent application of the law, as organizations often neglect loopholes to minimize compliance costs.

3.3. Lack of Global configuration

Data does not respect borders. While the DPDPA may be effective within a specific jurisdiction, it often fails to account for cross-border data flows. Differences in set of laws across countries create challenges for enforcement and allow organizations to exploit lenient arbitrage.

4. Challenges in Enforcement

4. 1. Source Constraints

Regulatory bodies tasked with enforcing the DPDPA often lack enough endowment and manpower. Investigating data breaches, auditing organizations, and addressing individual complaints require substantial resources, which are frequently unavailable.

4. 2. Limited Penalties

The penalties for non-compliance are often deficient to deter enormous corporations. For instance, multinational companies with vast revenues may view fines as insignificant compared to the earnings gained from exploiting personal data.

4.3. Reactive, Not positive

Enforcement is primarily reactive, focusing on breaches and complaints rather than preventing violations. This approach leaves a significant gap in ensuring positive compliance by organizations.

4.4. Lack of responsiveness Among Stakeholders

Many individuals are unaware of their rights under the DPDPA, and organizations often fail to fully understand their obligations. This lack of awareness reduces the efficacy of the Act in protecting personal data.

5. Emerging Threats to Data Privacy

5.1. Sophisticated Cyber attacks

The rise of sophisticated cyber attacks, including ransom ware and phishing, has highlighted the deficiency of current data protection procedures. The DPDPA's prominence on observance more security means organizations may meet the letter of the law while remaining vulnerable to breaches.

5.2. Mass Data Collection

With the proliferation of smart devices and online platforms, companies are collecting unparalleled amounts of data. The DPDPA struggles to legalize such mass data collection, more than ever when users unknowingly consent to data processing via opaque terms and circumstances.

5.3. Data Brokers and Shadow Profiles

Data brokers collect extensive profiles of individuals by aggregating data from various sources, often without their knowledge or consent. The DPDPA offers limited mechanisms to address this practice, leaving individuals open to the elements of privacy violations.

5.4. Artificial Intelligence and Machine Learning

AI systems rely on vast datasets to function efficiently. The DPDPA often fails to address issues like biased data sets, lack of transparency in decision-making algorithms, and the potential misuse of AI for surveillance purposes.

6. Case Studies Highlighting Ineffectiveness

6.1. Cambridge Analytica Scandal

The Cambridge Analytica scandal exposed how individual data could be harvested and demoralized for political gain, often without individuals' consent. Despite existing data protection laws, the incident exposed significant gaps in oversight and enforcement.

6.2. Equifax Data Breach

The 2017 Equifax breach compromised the personal information of over 140 million individuals. The breach highlighted the inadequacy of compliance-focused approaches, as the company had outwardly adhered to regulations yet failed to execute forceful security measures.

6.3. GDPR vs. DPDPA

The General Data Protection Regulation (GDPR) in the European Union is often cited as a more robust framework compared to the DPDPA. However, even the GDPR faces criticism for enforcement challenges and its limited ability to address global data privacy issues, reflecting similar shortcomings in the DPDPA.

7. Recommendations for Improvement

7.1. Regular Updates to Legislation

Data protection laws must evolve in tandem with technological advancements. Regular reviews and updates to the DPDPA can ensure it remains relevant and effective.

7.2. Stronger Enforcement Mechanisms

Regulatory bodies should be equipped with sufficient resources to enforce the law effectively. Penalties for non-compliance should be considerable enough to act as a deterrent.

7.3. Intercontinental Cooperation

Harmonizing data protection laws across jurisdictions can address challenges related to cross-border data flows. global agreements and mutual enforcement mechanisms are essential.

7.4. Augmented knowledge and Education

Public campaigns and training programs can help individuals understand their rights and organizations their obligations. This increased awareness can drive better compliance and advocacy for stronger laws.

7.5. Focus on Security

The DPDPA should prioritize robust data security measures alongside compliance. Encouraging organizations to adopt advanced encryption, regular audits, and incident response plans can diminish risks.

7.6. AI-Specific Regulations

The rise of AI demands tormented regulations addressing issues like algorithmic transparency, bias, and accountability. Integrating these into the DPDPA can ensure it remains effective in the AI era.

8. Conclusion

The Digital Privacy Data Protection Act, while a step in the right direction, falls short of effectively addressing the complexities of data privacy in the modern world. Its structural weaknesses, enforcement challenges, and inability to keep pace with emerging threats undermine its efficacy. To truly protect individuals in an increasingly data-driven society, the DPDPA must experience noteworthy reform, supported by stronger enforcement, international cooperation, and a focus on evolving technologies. Only then can it achieve its goal of safeguarding personal data in a rapidly altering digital setting.

WHITE BLACK
LEGAL