



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

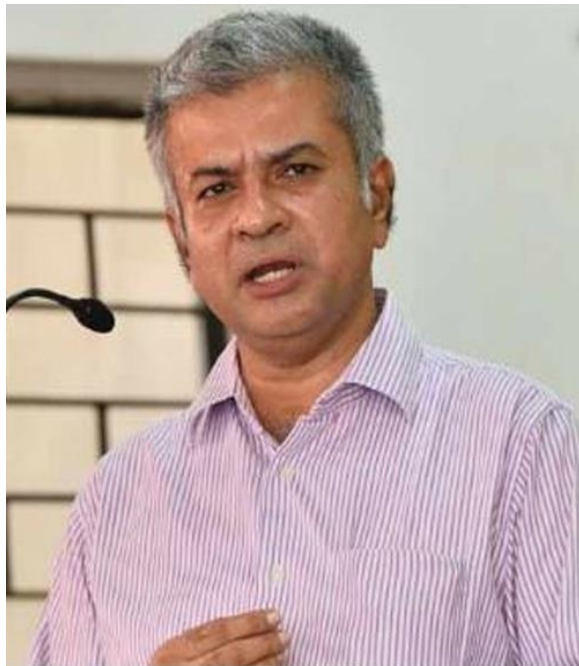
No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

– 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 Procurement from the World Bank.

in Public

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

A Constitutional perspective of Digital Personal Data Protection Act, 2023 (DPDPA)

By- Dr. C. Usha

Chennai Dr. Ambedkar Government Law College, Pattaraiperumpudur, Thiruvallur

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.” — Edward Snowden

Abstract:-

The Digital Personal Data Protection Act, 2023 (DPDPA) marks a pivotal moment in India's legislative landscape, aiming to regulate the processing of digital personal data and safeguard individuals' privacy rights. From a constitutional perspective, the DPDPA embodies the principles enshrined in the Indian Constitution, particularly the right to privacy as articulated by the Supreme Court. This research paper critically examines the constitutional foundations of the DPDPA, assessing its alignment with fundamental rights, separation of powers, and the principles of proportionality and reasonableness. Additionally, it analyzes the implications of the DPDPA on digital governance, data sovereignty, and India's position in the global data economy. By exploring the constitutional dimensions of the DPDPA, this paper aims to contribute to the ongoing discourse on privacy legislation and digital governance in India.

1. INTRODUCTION

In an era characterized by pervasive digitalization and ubiquitous data collection, the protection of personal data has emerged as a pressing concern worldwide. India, as a global leader in information technology and digital innovation, recognized the need for comprehensive legislation to address the challenges posed by the digital ecosystem while safeguarding individuals' privacy rights. The Digital Personal Data Protection Act, 2023 (DPDPA) represents a landmark legislative effort to regulate the collection, processing, and sharing of digital personal data within the country.

The background of the DPDPA traces back to the landmark judgment of the Supreme Court of India in the case of Justice K.S. Puttaswamy (Retd) vs. Union of India (2017), which recognized the right to privacy as a fundamental right under the Indian Constitution. This pivotal ruling laid the constitutional groundwork for the formulation of

a robust data protection framework in India. Subsequently, the government constituted a Committee of Experts on Data Protection, chaired by Justice B.N. Srikrishna, to draft a comprehensive data protection law.

The DPDPA, introduced in Parliament in 2023, builds upon the recommendations of the Srikrishna Committee and aims to address the growing concerns surrounding data privacy and security. One of the key objectives of the DPDPA is to establish a legal framework for the processing of digital personal data, ensuring transparency, accountability, and individual rights protection. The Act applies to both public and private entities engaged in the collection, storage, processing, or sharing of digital personal data, thereby encompassing a wide range of stakeholders within its ambit.

From a constitutional perspective, the DPDPA is anchored in the fundamental rights guaranteed by the Indian Constitution, particularly the right to privacy as articulated in Article 21. The Act seeks to strike a balance between individual privacy rights and legitimate state interests, incorporating principles of necessity, proportionality, and reasonableness in data processing activities. Additionally, the DPDPA delineates the roles and responsibilities of various stakeholders, including data fiduciaries, data processors, and the Data Protection Board of India, established to oversee compliance and enforcement.

In the subsequent sections of this research paper, we will delve deeper into the constitutional dimensions of the DPDPA, analyzing its provisions in light of constitutional principles and judicial interpretations. Furthermore, we will examine the background and evolution of the Act, contextualizing it within the broader landscape of digital governance and data protection in India. Through this analysis, we aim to provide a comprehensive understanding of the constitutional framework underpinning the DPDPA and its implications for privacy rights and

digital governance in India.

2. CONSTITUTIONAL PROVISIONS FOR DATA PROTECTION

Data protection in India is intricately linked to constitutional provisions that safeguard fundamental rights, including the right to privacy. These constitutional provisions lay the groundwork for legislation such as the Digital Personal Data Protection Act, 2023 (DPDPA) and shape the legal framework governing data protection in the country.

2.1 Constitutional Provisions

The Indian Constitution guarantees several fundamental rights that are pertinent to data protection. Article 21, often referred to as the "Right to Life and Personal Liberty," has been interpreted expansively by the judiciary to include the right to privacy. This right has been upheld as intrinsic to the protection of personal autonomy and dignity. Additionally, Article 19(1)(a) provides for the freedom of speech and expression, which encompasses the right to informational privacy. Together, these constitutional provisions form the bedrock for data protection legislation in India, emphasizing the importance of individual autonomy, dignity, and freedom from unwarranted state intrusion.

2.2 Judicial Precedents relating to privacy

Judicial precedents in India have played a significant role in shaping the discourse around privacy rights and data protection. The landmark judgment in Justice K.S. Puttaswamy (Retd) vs. Union of India (2017), commonly known as the "Privacy Judgment," reaffirmed the right to privacy as a fundamental right under the Indian Constitution. The Supreme Court held that privacy is an essential attribute of personal liberty and intrinsic to the exercise of other fundamental rights. This seminal decision laid the foundation for legislative measures such as the DPDPA, providing constitutional legitimacy to data protection efforts in India.

Furthermore, the judiciary has consistently emphasized the need to strike a balance between individual privacy rights and legitimate state interests. In cases involving surveillance and data collection by the state, courts have applied principles of proportionality and necessity to assess the constitutionality of such measures. For

instance, in *People's Union for Civil Liberties (PUCL) vs Union of India* (1996), the Supreme Court outlined safeguards for interception of communication on grounds such as national security, emphasizing the importance of necessity and proportionality in state action.

2.3 Reports and commissions

Various reports and commissions have also contributed to the discourse on data protection and privacy in India. The Report of the Committee of Experts on Data Protection, chaired by Justice B.N. Srikrishna, played a pivotal role in shaping the contours of the DPDPA. The committee's recommendations provided valuable insights into the challenges posed by the digital ecosystem and proposed comprehensive measures to address them. Additionally, reports from parliamentary committees, such as the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, have provided valuable inputs for refining data protection legislation in India.

Moreover, international frameworks and reports, such as the General Data Protection Regulation (GDPR) of the European Union, have influenced discussions on data protection standards and best practices. While not binding, these frameworks serve as reference points for policymakers and legislators seeking to align India's data protection regime with global norms.

3. CONSTITUTIONAL ANALYSIS OF IMPORTANT PROVISIONS OF DPDPA, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) represents a significant legislative effort to regulate the processing of digital personal data in India while upholding constitutional principles and safeguarding fundamental rights. A constitutional analysis of key provisions of the DPDPA sheds light on the alignment of the legislation with constitutional mandates and principles.

One of the fundamental aspects of the DPDPA is its adherence to the right to privacy enshrined in Article 21 of the Indian Constitution. The Act recognizes the importance of

individual autonomy and dignity by placing restrictions on the processing of personal data without consent. Section 3 of the DPDPA stipulates that personal data may only be processed for lawful purposes with the consent of the individual. This provision reflects the constitutional imperative to protect individuals from unwarranted intrusion into their private lives and underscores the principle of informational self-determination.

Moreover, the DPDPA incorporates principles of fairness and transparency, which are inherent in the constitutional scheme. Section 8 of the Act requires data fiduciaries to provide individuals with clear and concise notices regarding the processing of their personal data. This provision ensures that individuals are adequately informed about how their data is being used, thereby promoting transparency and accountability, which are essential components of a democratic society governed by the rule of law.

Another crucial aspect of the DPDPA from a constitutional standpoint is its provisions relating to data security and breach notification. Article 19(1)(a) of the Constitution guarantees the freedom of speech and expression, which includes the right to seek, receive, and impart information. The DPDPA recognizes the importance of safeguarding data against unauthorized access or disclosure to preserve individuals' freedom of expression. Sections 26 and 27 of the Act impose obligations on data fiduciaries to implement security safeguards and notify individuals in the event of a data breach. These provisions not only protect individuals' privacy but also uphold their right to access information without fear of unauthorized surveillance or censorship.

Furthermore, the DPDPA incorporates mechanisms for the redressal of grievances and enforcement of rights, in line with constitutional principles of access to justice and effective remedy. Section 34 of the Act empowers individuals to seek compensation for any harm caused by the processing of their personal data in violation of the provisions of the Act. This provision ensures that individuals have meaningful recourse in case of data misuse or privacy violations,

thereby strengthening the rule of law and promoting accountability.

Additionally, the DPDPA recognizes the importance of regulatory oversight in ensuring compliance with data protection standards, which is consistent with constitutional principles of checks and balances. The establishment of the Data Protection Board of India under Section 37 of the Act provides for an independent regulatory authority tasked with monitoring compliance, adjudicating disputes, and imposing penalties for non-compliance. This institutional framework ensures that data protection laws are effectively enforced, thereby promoting the rule of law and protecting individuals' rights in the digital sphere.

The Digital Personal Data Protection Act, 2023, reflects a constitutional commitment to protecting individual privacy and promoting transparency, accountability, and access to justice in the digital age. By incorporating key constitutional principles and safeguards, the DPDPA seeks to strike a balance between the imperatives of data-driven innovation and the protection of fundamental rights, thereby laying the foundation for a robust and rights-respecting data protection regime in India.

4. RIGHT TO PRIVACY VS. RIGHT TO INFORMATION - CONSTITUTIONAL APPROACH

The intersection between the right to privacy and the right to information represents a nuanced constitutional challenge that requires a careful balancing of competing interests and values. Both rights are considered integral components of a democratic society governed by the rule of law, yet they may come into tension in certain contexts, particularly in the realm of data protection and access to information.

At the heart of the debate lies the right to privacy, which is enshrined in Article 21 of the Indian Constitution as a fundamental right essential to human dignity and autonomy. The Supreme Court has recognized the right to privacy as encompassing the right to be left alone, the right to control one's personal information, and the right to make autonomous choices free from unwarranted interference. This right finds expression in various judicial pronouncements, including the landmark judgment in *Justice K.S. Puttaswamy (Retd)

vs. Union of India*, where the Court affirmed the constitutional protection afforded to individual privacy against state intrusion.

On the other hand, the right to information is recognized as a derivative of the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The right to information empowers citizens to access government records and information, thereby fostering transparency, accountability, and informed decision-making. The enactment of the Right to Information Act, 2005 (RTI Act) was a significant legislative step towards promoting transparency and accountability in governance by providing citizens with a mechanism to access government information.

However, the exercise of the right to information must be balanced against the right to privacy, particularly concerning the processing and disclosure of personal data. The proliferation of digital technologies and the collection of vast amounts of personal data have raised concerns about privacy infringement and data misuse. While the right to information is crucial for holding governments and public authorities accountable, it must be exercised in a manner consistent with privacy rights and data protection principles.

The Digital Personal Data Protection Act, 2023 (DPDPA) seeks to reconcile the right to privacy with the right to information by establishing a framework for the lawful processing and disclosure of personal data. The Act imposes obligations on data fiduciaries to obtain consent before processing personal data and to implement security safeguards to protect against unauthorized access or disclosure. At the same time, the Act recognizes the importance of transparency and accountability by requiring data fiduciaries to provide individuals with clear and concise notices regarding the processing of their data.

Moreover, the DPDPA incorporates provisions for the disclosure of information in the public interest while safeguarding individual privacy. Section 43 of the Act permits the disclosure of personal data for journalistic purposes, subject to certain conditions and safeguards. This provision strikes a balance between the right to privacy and the right to

freedom of expression by allowing for the responsible dissemination of information in the public interest.

Nevertheless, challenges remain in reconciling the right to privacy with the right to information, particularly in the context of emerging technologies such as artificial intelligence and big data analytics. The collection and analysis of vast amounts of personal data for various purposes raise complex ethical and legal questions regarding consent, transparency, and accountability. Regulatory frameworks such as the DPDPA play a crucial role in addressing these challenges by establishing clear rules and standards for the processing and disclosure of personal data while upholding constitutional values and principles.

The constitutional approach to balancing the right to privacy with the right to information requires a nuanced understanding of the competing interests and values at stake. While both rights are essential for democracy and good governance, their harmonization requires careful deliberation and the enactment of appropriate legal frameworks that uphold individual rights while promoting transparency, accountability, and informed decision-making in the digital age.

5. BALANCING PRIVACY RIGHTS WITH STATE INTERESTS THROUGH A LEGISLATIVE FRAMEWORK

The delicate balance between privacy rights and state interests lies at the core of legislative efforts aimed at regulating the processing and disclosure of personal data. While privacy rights are fundamental to individual autonomy and dignity, state interests encompass various objectives such as national security, law enforcement, and public welfare. Achieving a harmonious equilibrium between these competing interests requires a comprehensive legislative framework that ensures the protection of privacy rights while enabling legitimate state activities.

At the outset, it is essential to recognize that the state has a legitimate interest in accessing certain types of personal data for purposes such as national security, crime prevention, and public health. However, such access must be subject to strict legal safeguards and oversight mechanisms to prevent abuse and ensure accountability. Legislative frameworks play a crucial role in delineating the scope of state access to personal data and establishing clear rules and

procedures for its lawful processing and disclosure.

The Digital Personal Data Protection Act, 2023 (DPDPA) represents a significant legislative endeavor to balance privacy rights with state interests in the Indian context. The Act recognizes the importance of protecting individual privacy while also acknowledging the legitimate needs of the state to access personal data for specific purposes. To achieve this balance, the DPDPA incorporates several key provisions aimed at safeguarding privacy rights while enabling lawful state activities.

One of the primary mechanisms for balancing privacy rights with state interests is the establishment of legal bases for the processing of personal data. Under the DPDPA, data fiduciaries are required to obtain valid consent from individuals before processing their personal data, except in cases where processing is necessary for specified purposes such as compliance with a legal obligation or the performance of a task carried out in the public interest. This provision ensures that individuals retain control over their personal data while allowing for lawful state activities that serve the public good.

Moreover, the DPDPA imposes stringent obligations on data fiduciaries to implement security safeguards to protect personal data from unauthorized access, disclosure, or misuse. By establishing robust data protection standards, the Act aims to safeguard privacy rights while also enhancing trust and confidence in the digital ecosystem. These security measures are essential for mitigating the risks associated with state access to personal data and ensuring that such access is justified and proportionate to the legitimate objectives pursued by the state.

In addition to protecting privacy rights, the DPDPA also incorporates provisions aimed at promoting transparency and accountability in state activities involving personal data. The Act requires data fiduciaries to provide individuals with clear and concise notices regarding the processing of their data, including the purposes for which it is being processed and the entities to which it may be disclosed. By enhancing transparency, individuals are empowered to make informed decisions about the use of their personal data and hold both data fiduciaries and state authorities accountable for their actions.

Furthermore, the DPDPA establishes robust mechanisms for oversight and redressal to address violations of privacy rights by state actors. The Act empowers the Data Protection Authority (DPA) to monitor compliance with data protection obligations, conduct inquiries into alleged violations, and impose penalties for non-compliance. Additionally, the Act provides individuals with the right to seek compensation for damages arising from the unlawful processing of their personal data by state authorities, thereby ensuring effective redressal mechanisms for privacy violations.

Balancing privacy rights with state interests through a legislative framework requires careful deliberation and the adoption of measures that uphold constitutional values while enabling legitimate state activities. The Digital Personal Data Protection Act, 2023, represents a significant step towards achieving this balance by incorporating provisions aimed at safeguarding privacy rights, promoting transparency and accountability, and establishing mechanisms for oversight and redressal. By striking a delicate equilibrium between privacy rights and state interests, the Act seeks to foster trust and confidence in the digital ecosystem while preserving fundamental rights and freedoms in the digital age.

6. CONCLUSION

In conclusion, the Digital Personal Data Protection Act, 2023, represents a significant milestone in India's legislative landscape, aiming to strike a delicate balance between protecting privacy rights and accommodating legitimate state interests. Through its

comprehensive framework, the Act seeks to safeguard individual autonomy and dignity while acknowledging the necessity of state access to personal data for purposes such as national security and public welfare. By establishing clear rules and procedures for the processing and disclosure of personal data, the Act enhances transparency, accountability, and trust in the digital ecosystem. Through mechanisms such as valid consent, security safeguards, and oversight by the Data Protection Authority, the Act ensures that privacy rights are respected and upheld, even in the face of state activities. Moreover, the Act promotes a culture of data protection by empowering individuals to exercise greater control over their personal data and providing them

with avenues for redressal in case of privacy violations. By fostering a robust data protection regime, the Act not only safeguards individual privacy but also lays the foundation for a thriving digital economy built on trust and confidence.

However, the effectiveness of the DPDPA ultimately depends on its implementation and enforcement. It is imperative for stakeholders, including data fiduciaries, state authorities, and civil society organizations, to collaborate actively in ensuring compliance with the Act's provisions and holding accountable those who violate privacy rights. In essence, the DPDPA represents a critical step forward in aligning India's data protection framework with constitutional principles and international best practices. As technology continues to evolve and shape our digital world, the Act serves as a crucial safeguard for preserving fundamental rights and freedoms in the digital age.

7. REFERENCE

Books:

1. Dr. J. N. Pandey, Constitutional Law of India, (51st edition)
 2. Narendra Kumar, Constitutional Law of India, (9th edition)
 3. M.P. Jain, Indian Constitutional law, (7th edition)
 4. Madhavi Goradia Divan, Facets of Media Law, (2nd edition)
 5. Paras Diwan, Law of Marriage and Divorce, (3rd edition)
 6. Dr. Avtar Singh, College Law Dictionary, (2nd edition)
 7. Dr. Singh Avtar, Principles of The Law of Evidence, (21st edition)
8. Sharma S.K., Privacy Law- A Comparative study, (11th edition) Reports:
1. National Law Commission India: 69th Report on Right To Privacy Websites:
 1. <https://www.manupatra.com>
 2. <https://www.wordpress.com>
 3. <https://www.indiankanoon.org>
 4. <https://www.indianexpress.com>
 5. <https://www.thehindu.com>
 6. <https://timesofindia.com>
 7. <https://www.theweek.in>

8. <https://www.britannica.com>
9. <https://scroll.in>
10. <https://www.linklaters.com>
11. <https://www.legalserviceindia.com>
12. <https://digitalindia.gov.in>



WHITE BLACK
LEGAL