



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, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DATA PROTECTION AND HUMAN RIGHT TO PRIVACY: A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - DR SATISH CHANDRA & VIBHA

Abstract

As digital technologies have rapidly developed, so has the collection and processing of personal data, leading to issues of privacy, surveillance, and misuse of the data. When the Supreme Court of India in the landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India, extended the Right to Privacy to Article 21 of the Constitution, it brought to the forefront the need for a full-fledged data protection regime in India. To address this, Parliament has, inter alia, passed the Digital Personal Data Protection Act, 2023 (DPDP Act) for the regulation of processing of digital personal data and protection of informational privacy. This paper discusses connection between Data Protection and the Human Right to Privacy, goal to understand the essential points mentioned in DPDP Act and assess the effectiveness of DPDP Act in protecting individual rights. The study concludes that the Act represents an important measure towards robust data governance and Data privacy, but raises concerns about the government's exceptions, independence of the regulatory regime and enforcement practices. The authors of the paper conclude that with the condition of the digital era, more reform must be done to guarantee a stronger protection of the rights to privacy.

Keywords

Data Protection, Right to Privacy, Digital Personal Data Protection Act, 2023, Informational Privacy, Human Rights, GDPR, Data Governance, Cyber Law, Constitutional Rights.

1.introduction

1.1 Introduction

Digital technology has developed at a fast rate, changing the way people, businesses and governments communicate and share information. With the rise of the smartphone, social networks, cloud computing, artificial intelligence, e-commerce and digital governance there has been an unprecedented expansion in the amount of data collected and processed, most of which is personal data. This includes data like name and address, financial information, biometric

information, health information and information about Internet use and behavior, which is collected and analyzed routinely for anything including service provision, business or public administration.¹

In today's digital age, data is a crucial asset and powerful enabler of innovation, growth and technology. Public and private sector organizations have turned to digital platforms to deliver public services, and the private sector has turned to personal data to customize public experiences, direct ads and create new products and services. Whilst these advances bring great advantages, they also create significant concerns when it comes to the protection of individual privacy and the individual's personal autonomy.²

With the widespread adoption of personal information, there are increased risks from data breaches and identity theft, cybercrime and unauthorized surveillance and misuse of sensitive information. There are many cases of large-scale data collection, in which people are not really aware or have a sense of real consent. With almost continuous technological developments comes the challenge of balancing innovation in technology and development of the economy with respect for privacy rights as the most basic foundation of the society. Thus, Data Protection has become a serious legal and human right concern globally and in India.

1.2 Statement of Research Problem

There has been no comprehensive law specifically for the protection of personal data in India for many years. Some provisions were already present in the Information Technology Act, 2000 and Information Technology Rules but they were also fragmented and insufficient to deal with the challenges of modern digital technologies and extensive data processing. There was a lack of a specific data protection legislation, which raised concerns about the use of personal data by the government or by private parties.

Rising data breaches, cyber attacks, data leakage and electronic information surveillance further raise concerns about informational privacy. In Justice K.S. Puttaswamy (Retd.) v. Union of India³, the Supreme Court recognized the right to privacy as constitutional and laid a foundation for the importance of introducing a comprehensive data protection law that can adequately

¹ Daniel J. Solove, *Understanding Privacy* 1–12 (Harvard Univ. Press 2008).

² Ministry of Electronics and Information Technology, Government of India, Digital India Programme, <https://www.digitalindia.gov.in>

³ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

protect the rights of the people in a digital era.

To address these concerns, Parliament has passed the Digital Personal Data Protection Act, 2023 (DPDP Act)⁴, aimed at governing the handling of digital personal data and enhancing data privacy in India. But doubts have been raised over whether or not the Act is sufficient to safeguard privacy rights. The law comes amid concerns over the breadth of government exemptions, independence of the regulators, surveillance capabilities, and the extent of the individual rights it covers. Thus, this study aims to critically analyse the effectiveness of the Digital Personal Data Protection Act, 2023 in achieving a balance between the interest of the State, the business and the citizens including protection of the fundamental right to privacy.

2. Review of Literature

Data protection and privacy have been the subject of much research, especially in the digital era of growth and technological innovation. The minds of various scholars, constitutional experts and the policymakers, have played a great role in understanding about the right of privacy and data governance.

In his book Indian Constitutional Law, MP Jain has discussed the development of Article 21 of the Constitution and how, over the years, privacy has been increasingly accepted by the judiciary as a part and parcel of personal liberty. He pinpoints the ways in which the constitutional courts have interpreted the concept of the fundamental right in such a manner that it incorporates the ideas of informational privacy and individual autonomy.⁵

V.N. Shukla mentions the linkages of fundamental rights, human dignity and personal liberty. His arguments give a valuable constitutional analysis about privacy protection, making a point that the right to liberty guaranteed by Article 21 is not only physical freedom but it is also pertaining to personal autonomy or privacy.⁶

One of the most important contributions to the data protection debate in India is the Justice B.N. Srikrishna Committee Report (2018). The Committee defined privacy as a basic right and proposed a comprehensive legislative package which sought to be based on the following

⁴ Digital Personal Data Protection Act, No. 22 of 2023, §§ 1–3, India Code (2023).

⁵ M.P. Jain, Indian Constitutional Law 1357–60 (8th ed. 2018).

⁶ V.N. Shukla, Constitution of India 312–15 (13th ed. 2017).

principles: consent, accountability, transparency, data minimisation and purpose limitation. The report provided the groundwork for the present data protection framework of India.⁷

Graham Greenleaf offers a thorough evaluation of the existing data protection framework in India and suggests that, although these laws are a step in the right direction, there are certain issues that need to be addressed in terms of enforcement, government exemptions and institutional independence. His contributions focus on the trade-offs between privacy and national security and governance goals.⁸

Daniel J. Solove is a leading privacy scholar, creating theoretical frameworks for explaining privacy in the digital age. Beyond secrecy, privacy harms include problems like surveillance, information aggregation, exclusion, and misuse of personal information, he says. His theories give a full set of elements to assess modern laws in the area of data protection.⁹

The book looks at the surveillance of personal data and their commercial exploitation by digital corporations through the work of Shoshana Zuboff, who coined the term “surveillance capitalism.” Her projects have shed light on the increasing influence of tech firms and how their data-collection practices threaten individual autonomy and democratic ideals.¹⁰

The available literature is a rich source of information on constitutional 297 rights to privacy, data governance and digital surveillance. There is a significant gap in research in the implementation of the Digital Personal Data Protection Act, 2023, and its efficacy in safeguarding informational privacy. There has been little scholarly evaluation of matters like governmental exemptions, the lack of independence of the Data Protection Board, surveillance issues, and compatibility of the Act in the light of constitutional principles laid down in the case of Puttaswamy. Thus, the DPDP Act, 2023 needs to be critically analyzed to evaluate if it sufficiently fortifies the safeguard of privacy as a basic human right in India's digital era.

⁷ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 21–35 (2018).

⁸ Graham Greenleaf, *India's New Data Protection Law: Progress and Problems*, 169 *Privacy Laws & Business International Report* 1, 2–5 (2023).

⁹ Daniel J. Solove, *Understanding Privacy* 75–103 (Harvard Univ. Press 2008).

¹⁰ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 93–120 (Profile Books 2019).

3. Objectives of the Study

1. To explore the idea of 'privacy as a human right'.
2. To study constitutional evolution of the concept of privacy in India.
3. Making an objective analysis of various salient features of Digital Personal Data Protection Act, 2023.
4. To be able to critically assess the effectiveness of the Act from the point of view that it protects personal data.
5. To make recommendations on strengthening the privacy protection in India.

4. Research Questions

1. Right to Privacy is a part of Article 21 of the Constitution of India or not?
2. Whether the DPDP Act, 2023 effectively protects informational privacy?
3. What is the key ingredients, strengths and weaknesses of the Act?
4. How is the Indian framework in line with international standards like GDPR?
5. Which reforms do you need to see to improve the protection of personal data?

5. Research Methodology

A Doctrinal/Analytical research methodology is used. The sources of information that have been used include books and journal articles, government reports, statutes, judicial decisions, committee reports, and online databases. The study discusses constitution, the Digital Personal Data Protection Act, 2023, and some key case laws concerning privacy rights. The GDPR is also analysed in comparison.

6. Discussion / Analysis

6.1 Rights for Data Protection

The concept of privacy is treated as a human right which safeguards the dignity, autonomy, liberty and individual freedom of the person. In today's digital age, there is a wealth of information that is gathered and processed on smart phones, social networking sites, e-commerce sites and government databases. For these reasons, data protection is an integral part of privacy protection. It may result in violation of personal information and could lead to the misuse of personal information and identity theft, discrimination and surveillance. It is therefore important for there to be legal protections allowing people to remain in control of their personal

information.¹¹

The international endorsement of privacy as a human right is evident in Article 12 of the Universal Declaration of Human Rights (UDHR) which outlaws interference with privacy, family, home and correspondence, except where it is justified in accordance with law. Likewise, the right to freedom from inhuman or degrading treatment in the ICCPR, article 17, is relevant as informational privacy has increasingly been relevant in today's digital society, in which personal information is collected, analysed, and disseminated by private and public entities.¹² Proper data protection laws are thus an essential component in protecting human rights and enabling trust in digital systems.

6.2 Development of Right to Privacy in India

Even in the Constitution of India, the Right to Privacy was not mentioned explicitly as a right of the people of India. Privacy jurisprudence was slowly built up by judicial interpretation. Similarly, in *M.P. Sharma v. Satish Chandra* the Supreme Court, albeit with a narrow perspective, recognised that unauthorised inroad had an impact on the personal liberty covered by Article 21.¹³ In *Kharak Singh v. State of Uttar Pradesh*, the Supreme Court also had a narrow interpretation but confirmed that unauthorised inroad would have an impact on the personal liberty covered by Article 21.¹⁴

In *Gobind v. State of Madhya Pradesh*, Supreme Court held that the right to privacy could be read into the right to personal liberty.¹⁵ Further, the Supreme Court in *R. Rajagopal v. State of Tamil Nadu* has introduced the concept of the “Right to be Let Alone” and held that the privacy of the individual could be protected against unauthorized disclosures of private information.¹⁶

Finally, in the landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court ruled that privacy is a fundamental right enshrined in Article 21 of the Constitution. The judgment underscored a natural link between privacy and human dignity, liberty, and autonomy and emphasized the significance of informational privacy in the digital era. This was a pivotal

¹¹ Daniel J. Solove, *Understanding Privacy* 1–15 (Harvard Univ. Press 2008).

¹² Universal Declaration of Human Rights art. 12, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

¹³ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

¹⁴ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

¹⁵ *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.

¹⁶ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

judgment that paved the way for the introduction of an laws related to data protection in India.¹⁷

6.3 Key highlights of the DPDP Act, 2023

Digital Personal Data Protection Act, 2023 is India's first large-scale law focusing on the protection of the Digital Personal Data. The Act covers digital personal data gathered in India and in some cases, data processed outside India, where services or goods are provided to an individual located within that country.⁹ The Act seeks to strike a balance between individuals' rights to privacy and the lawful interests of businesses and governmental authorities.

A one of the key features of the Act is because of consent centered handling. Data ¹⁸Fiduciaries are required to obtain informed and specific consent before processing personal information. The Act provides various rights to the Data Principals such as Access, Rights on Passport Information, Right of Correction and Erasure of Data, Right of Grievance Redressal, Right to nominate an Alternate Person to exercise the rights.¹⁹

The Act also makes requirements on Data Fiduciaries, including that they have appropriate data safeguards, proactively stop data breaches, and take reasonable steps to keep personal data accurate. The law also includes a provision for the Data Protection Board of India to investigate complaints and enforce penalties for non-compliance.

Additional safeguards put in place for children's data. It mandates parental consent that is verifiable and it puts limits on the monitoring of children's behavior, tracking and be-targeted advertent on children. Moreover, the Act allows cross-border transfers of personal data to countries approved by the Central Government and thus makes it easier to conduct business internationally and keep a regulatory check.¹²

7. Case Analysis

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) is one of the historic decisions that laid down the basis for privacy jurisprudence in India. The controversy had come up against Aadhaar and Verified Information Coding division of the UFE withholding the personal information. The real problem that Supreme Court was faced with was whether to regard the

¹⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁸ Id. §§ 18–28.

¹⁹ Digital Personal Data Protection Act, No. 22 of 2023, §§ 1–3, India Code (2023).

Right to Privacy as a fundamental right of the Constitution. It was a unanimous decision by all nine judges in the bench that privacy is a part of the right to life and personal liberty as guaranteed in Article 21. The Court highlighted the three dimensions of privacy: bodily integrity, personal autonomy and informational privacy. This judgment had a profound impact on the evolution of data protection legislation and ultimately contributed to the creation of the Digital Personal Data Protection Act (DPDP), 2023.²⁰

The Supreme Court has read the constitutionality of telephone tapping in *People's Union for Civil Liberties v. Union of India*, 1997. The Court found that it is a significant part of a person's private life to engage in telephone conversations and that such interceptions, without the person's consent, are an intrusion into their right to privacy. The Court acknowledged the State's authority to undertake surveillance in extraordinary cases but made certain that there were procedural guarantees to avoid arbitrary surveillance. The judgment bolstered privacy protection by making sure that surveillance actions continue to be subject to legal and procedural review.²¹

The *Auto Shankar Case* (popularly called *R. Rajagopal v. State of Tamil Nadu*) is a Supreme Court decision from the year 1994 which considered the “Right to be Let Alone” to be an intrinsic part of the right to privacy. The Court ruled that details regarding a person's family, marriage and private life are essential personal matters that cannot be published without his or her consent unless the information is already in the public domain as part of the information already in records. The judgment put forth significant safeguards against unauthorized sharing of personal data and played a crucial role in shaping the trajectory of privacy rights in India.²²

8. Findings

It has been found that due to judicial interpretations, privacy has now become a constitutional right in India with *Justice K.S. Puttaswamy (Retd.) v. Union of India*. As Informational Privacy has gained recognition, more and more attention is given to the need for effective legal mechanisms to protect Personal Data in an increasingly digital society. It is noteworthy that the Digital Personal Data Protection Act, 2023 is India's first specific law for regulating digital personal data processing and protection.

²⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

²¹ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

²² *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

The Act introduces important principles like consent-based processing, Accountability of Data Fiduciaries, Rights of Data Principals, Grievance Redressal Mechanisms, which add up to better protection of privacy. There are, however, a number of concerns in the study. Government agencies can receive broad exemptions to privacy protections that can lead to unnecessary surveillance. The somewhat lack of autonomy in DPIPWE raises questions about effective enforcement and accountability. Additionally, the public's awareness of privacy rights and the responsibilities for data protection are comparatively not high enough to be influential in how the law is put into practice. Overall, the Act is a step forward, but there are some legal and institutional issues.

9. Recommendations / Suggestions

Government exemptions must also be carefully circumscribed and judicially or independently reviewable to stop misuse of 'surveillance powers' within the ambit of the Digital Personal Data Protection Act, 2023. More independence should be given to the Data Protection Board for fair implementation of privacy rights and data protection duties.

There is a need for greater protection of sensitive private information, such as health, biometric, financial or genetic data, as these types of information carry greater risks when it comes to abuse. Other rights, like the right to move the data, the right to object the treatment and the safeguards against automated decisions should also be added to give individuals more power on their personal data.

There is a need to encourage public awareness-raising campaigns and digital literacy programs to educate citizens about their privacy rights and responsibilities in the digital world. Companies and government bodies should embrace privacy-by-design, bolster cybersecurity protocols, and regularly assess their security to safeguard against responsible data handling at the organizational level. These changes will have a substantial impact on strengthening the data protection regime in India, making it more rights-centric and robust.

10. Conclusion

With the passing of the Digital Personal Data Protection Act, 2023, India has taken a significant leap forward in its attempt to put in place a robust framework for data protection and privacy

governance. The adoption of the law underscores the increasing appreciation of privacy as a key fundamental constitutional right and the growing need to safeguard personal data in a fast digitalized society. The Act aims to provide a well-rounded framework for the regulation of the collection and use of personal data by introducing provisions relating to consent-based processing, accountability of Data Fiduciaries, rights of Data Principals and grievance redressal mechanism.

The study is proof that the Act is a significant measure in the direction of enhancing informational privacy and enabling good data governance. But, some other issues remain such as the extensive governmental exemptions, Data Protection Board's autonomy, sensitive personal data and enforcement. The effectiveness of this legislation to protect privacy rights and hold to account could be influenced by such issues.

Moreover, safeguarding information, as more and more digital technologies advance, will continue to be an important element of the individual's liberty, dignity and autonomy. Hence, there will be a need for ongoing legislative scrutiny, higher institutional protection standards, public education, and implementation mechanisms to cope with issues of privacy. A stronger and rights-centric data protection regime will not only fortify constitutional protections but also help build public trust in the data protection regime, facilitate digital inclusion, and promote responsible technological innovation in India's burgeoning digital landscape.

References / Bibliography

Books

Duggal, Pavan. *Cyber Law in India*. 2nd ed. New Delhi: Saakshar Law Publications, 2017.

Jain, M.P. *Indian Constitutional Law*. 8th ed. Gurugram: LexisNexis, 2018.

Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray Publishers, 2013.

Shukla, V.N. *Constitution of India*. 13th ed. Lucknow: Eastern Book Company, 2017.

Solove, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

Statutes and Legislations

Constitution of India, 1950.

Digital Personal Data Protection Act, 2023.

Information Technology Act, 2000.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

Committee Reports and Government Publications

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

Ministry of Electronics and Information Technology, Government of India, Digital India Programme.

Report of the Committee of Experts on Data Protection Framework for India (2018).

Journal Articles

Greenleaf, Graham. "India's New Data Protection Law: Progress and Problems." *Privacy Laws & Business International Report*, No. 169 (2023).

Solove, Daniel J. "A Taxonomy of Privacy." *154 University of Pennsylvania Law Review* 477 (2006).

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *4 Harvard Law Review* 193 (1890).

Kuner, Christopher. "The Internet and the Global Reach of EU Law." *13 Columbia Journal of European Law* 273 (2007).

Cases

Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

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

Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

Websites

Ministry of Electronics and Information Technology, Government of India,
<https://www.meity.gov.in>

India Code, <https://www.indiacode.nic.in>

United Nations Human Rights Office of the High Commissioner, <https://www.ohchr.org>

European Commission, <https://commission.europa.eu>

PRS Legislative Research, <https://prsindia.org>



WHITE BLACK
LEGAL