



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



WHITE BLACK
LEGAL.

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.

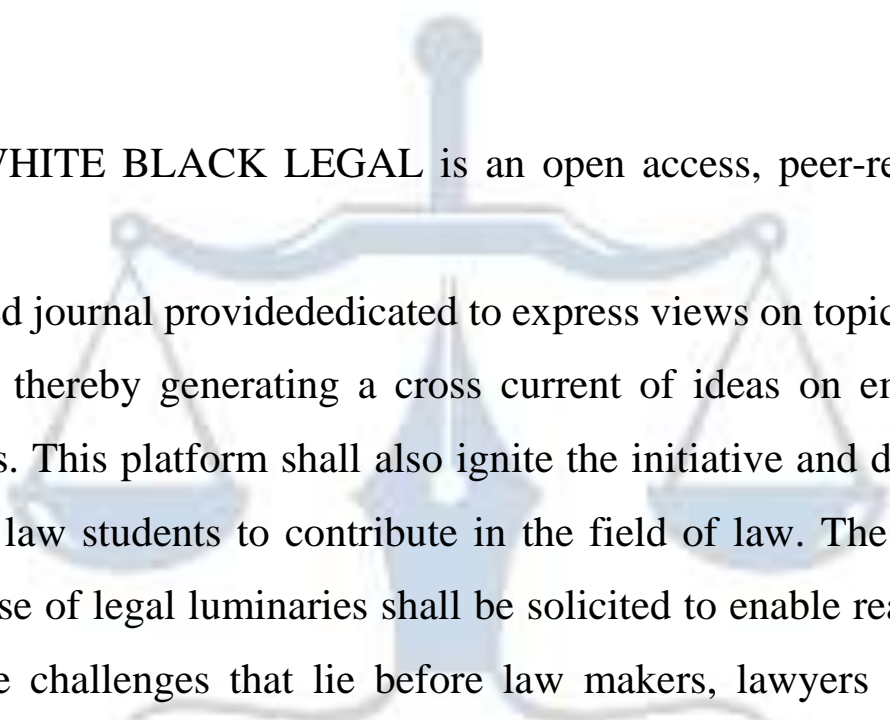


Subhrajit Chanda

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 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 COMPARATIVE ANALYSIS: WHY INDIA NEED STRICT PRIVACY LAWS IN THIS DIGITAL AGE

AUTHORED BY – PREETI & LAKSHAY SONKER

UNIVERSITY OF DELHI

ABSTRACT

In this article the writer tried to explain the consequences faces by the individuals for the violation of their personal liberty which is very important part for every individual to live life free and without any fear. Recently the Supreme Court has been rejected the plea of WhatsApp –Meta against Competition commission of India for probing the privacy policy of 2021. In India the landmark judgement under “K.S Puttaswamy Versus Union of India in 2017 declared that Right to Privacy is Fundamental Right. In India it is an intrinsic part of individual’s life and liberty in Indian Constitution. So here the writer tried to explain the concept of privacy and need to regulate strict digital framework on privacy and tried to compare the legal provisions with other countries with some important judgements.

INTRODUCTION

Many constitutions around the world include the right to privacy as a basic right. The concept of the right to privacy is complex. In today's society, the right to privacy is recognised by law and customary use. One of the most fundamental and widely recognised personal rights is the right to privacy. The Universal Declaration of Human Rights and the International Covenants on Civil and Political Rights both include references to the right to privacy. The right to privacy is one of the most basic aspects of life.

There has been a growing collection of international and regional laws and regulatory frameworks dealing to the protection of personal data since the late 1970s. Personal information must be collected or obtained honestly and legitimately, according to the law.

Personal information might include hobbies, interests, and activities, as well as educational, family, and educational records, correspondence, medical data, and financial records. This increased usage of personal data has numerous advantages, but it also has the potential to cause

numerous issues. Technological advancements have made personal information more accessible and communicable.

Between data protection and the right to privacy, there is an unbreakable conflict. In the digital age, it is a critical tool of healthy democratic governance that protects an individual's privacy. Despite global knowledge and acceptance of data protection, there is a lack of legal and institutional frameworks, processes, and infrastructure to support data and privacy rights protection.

Privacy as a concept:

The concept of data protection regulation is well-known throughout the world. The concepts "privacy" and "right to privacy"¹ is difficult to define. It has been used in a variety of ways in various situations. The right to privacy is often used as right to be left alone. A formal relationship between groups or individuals is known as privacy. Privacy is a value, a cultural state, or a condition aimed at individual and community self-realization that varies by society. The right to freedom of speech and expression is guaranteed by the Indian Constitution, which states that a person is free to express his or her will and conscience. A person's life and personal liberty are protected by the law and can only be taken through legal means. The European Union has a highly developed data privacy regulation. Personal information can only be collected in full accordance with European regulations for legal purposes.

Protection of personal information and privacy:

Data protection dictates that information on a person should not be made available to other people or organisations on an automatic basis. Everyone should be able to exercise a significant degree of control and usage over his or her data. Data protection refers to the legal safeguards in place to avoid the misuse of personal information obtained through electronic means.

It served as a tool for the implementation of administrative, technical, and physical deterrents to protect personal data. Data security and privacy are inextricably linked. Individual data, such as name, address, and phone number, is frequently available at many locations, such as schools, colleges, and banks, as well as on several websites. The disclosure of this information to

¹ Right to privacy: The Right to privacy is given under Article 21 of the Indian Constitution under “protection of life and personal liberty”.

interested parties will amount to an invasion of an individual's privacy, similar to receiving endless marketing calls.

What is the definition of personal data?

Personal data refers to any information that can be used to identify or contact a specific natural person or individual. Personal data refers to a collection of data that when linked or gathered together can be used to identify a specific person. For instance: person's names and surnames, person's home addresses and email addresses.

Data Protection Concept:

Data protection is a legal term that refers to a law that protects your personal information. In modern societies, this regulation allows us to have control over our data and safeguard it from misuse. Data protection rules regulate and limit the operations of businesses and government agencies. These institutions have repeatedly demonstrated that, absent any rules restricting their behaviour, they will gather everything, mine everything, keep everything, and share and utilise it with others without informing us anything.

What is the Need for Data Protection?

When a person buys anything online, uses a service, pays taxes, enters into a contract, uses a service, registers for email, or goes to the doctor, they must provide personal information. Companies and organisations are connecting the data and information without interacting with people, even if they are unaware of it. Citizens and customers can only have faith in both businesses and governments because of statutory laws governing data protection procedures which aid in successful legislation to reduce corporate spying and data exploitation. During the 1960s², as information technology capabilities grew around the world, corporations and governments began to store personal information in databases. Anyone can search these databases, and they can be changed, altered, and shared with other organisations throughout the world. People began to be concerned about what would happen to their data once it was processed or collected and made available to the public. Data protection principles were formed through different national and international forums, in response to the fast growing concerns and inquiries from the public.

² Information Technology (History): Available at 'Wikipedia'.

According to reports, 90% of the data on the planet today has been processed or collected in the last two years. As of January 2020, 107³ nations throughout the world have passed data protection laws, legislation, or were in the process of enacting them.

The world appeared to be a totally different place when numerous data protection rules were created. The following benefits are:-

- Personal data should be gathered and obtained in a lawful, fair, and transparent manner.
- Personal data processing and collection should be relevant, adequate, and limited to the reasons for which it is to be obtained.
- Measures should be taken to ensure that data are accurate and complete.
- Reasonable security or safeguards should be in place to protect the data from loss, destruction, use, leakage, disclosure, modification, and unauthorised access.
- No data, use, or other processes should be kept secret.
- Individuals whose data is gathered or obtained must have a set of rights that allow them to govern their data and its processing.
- Those who are using or collecting that data must be held accountable and guarantee that the above standards are followed, as well as the laws that entrench these principles.

The Indian Legal System's Approach to Privacy and Data Protection:

Article 19⁴ of India's Constitution guarantees freedom of speech and expression, whereas Article 21 guarantees the Right to life and liberty⁵. These Articles have an impact on the right to privacy, which is protected under Part III of the Constitution as a basic right⁶. The right to privacy as a basic right is addressed in a number of cases. The characteristics of this approach have been linked to new data protection aspects. The relationship between privacy and data protection is inextricably linked. The right to data protection is concerned with personal information. Individual rights arose naturally, and hence the right to privacy arose naturally as well.

³Data protection laws available at “Endpointprotector.com” and “Data protection Legislation Around the world 2021”.

⁴ Article 19: The Article 19 is a Fundamental right of the Indian Constitution from the bare Act.

⁵ Article 21: The Article 21 of the Indian Constitution is a Fundamental Right under “Protection of life and liberty”, content available at the Constitution of India’s bare Act.

⁶Part third is fundamental right and content available at the Constitution of India’s bare Act.

A. M.P. SHARMA AND OTHERS VERSUS SATISH CHANDRA⁷:

The case involved the search and seizure of papers from various 'DALMIA' group entities as a result of inquiries into their business dealings. The district Magistrate issued warrants after receiving a FIR, and searches were carried out as a result. The Constitutional legitimacy of the searches was challenged in writ petitions before the Supreme Court on the basis that they breached their fundamental rights under Articles 19(1) (f)⁸ and 20 (3)⁹—protection against self-incrimination. The Supreme Court concluded in 'M.P. SHARMA VERSUS SATISH CHANDRA' that the drafter of the Constitution did not intend to subject the power of search and seizure to a fundamental right of privacy. They said that the Constitution lacks language equivalent to that found in the Fourth Amendment of the United States Constitution, and that there is no rationale for imposing the concept of a fundamental right to privacy in searches and seizures through a 'strained construction'.

B. KHARAK SINGH VERSUS STATE OF UTTAR PRADESH AND OTHERS¹⁰:

The applicable rules allowing police to undertake domiciliary visits to "habitual criminals or persons likely to become habitual criminals" were deemed illegal by India's Supreme Court. 'KHARAK SINGH's house was frequently visited by the police at unusual hours, waking him up from his slumber. The Court reasoned that the visits violated the Petitioner's right to life, which may only be limited by law, not by executive order such as the Uttar Pradesh Police Regulations. The Petitioners' contention that the shadowing of chronic criminals infringed on his right to privacy was dismissed by the Court since this right was not recognised as a basic right in India's Constitution. The other part of the verdict was overturned in August 2017 in the landmark case 'PUTTASWAMY VERSUS INDIA,' in which a nine-judge Supreme Court bench unanimously decided that the right to privacy is a basic right under the Indian Constitution.

C. GOVIND VERSUS STATE OF MADYA PRADESH AND ANOTHERS:

Similar to KHARAK SINGH VERSUS STATE OF UTTAR PRADESH, GOVIND questioned the legality of Madhya Pradesh Police Regulations relating to surveillance, including

⁷ Aforesaid Case: M.P. SHARMA AND OTHERS VERSUS SATISH CHANDRA: Available at "Indiainkanoon.com".

⁸Article 19(1) (f) referred from the bare act of the Constitution of India.

⁹ Article 20(3) referred from the bare act of the Constitution of India.

¹⁰ Aforesaid case: 'KHARAK SINGH VERSUS STATE OF UTTAR PRADESH AND OTHERS, GOVIND VERSUS STATE OF MADYA PRADESH AND OTHERS. ', taken from the 'INDIANKANOON'.

domiciliary visits. GOVIND claimed that he was under police observation as a result of false accusations made against him. The Supreme Court dismissed the appeal, but recommended that the Madhya Pradesh Police Regulations be revised, stating that they were "dangerously close to unconstitutionality".

D. K.S. PUTTASWAMY VERSUS UNION OF INDIA¹¹:

Concerns about privacy were raised before the Supreme Court in the case of "K.S. PUTTASWAMY CASE" where the "AADHAR" card scheme was at issue. It was challenged on the grounds that the gathering and compilation of citizens' biometric and demographic data for other purposes constitutes a violation of Article 21's basic right. The right to privacy, according to the Supreme Court, is inextricably linked to the human element and is at the heart of human dignity. As a result, the right to privacy was declared to be a basic right guaranteed by Article 21 of the Indian constitution.¹²

The Supreme Court's decision in this case defined privacy as a right that should be protected. These arguments lead to an emphasis on the actual harm that a person suffers as a result of a breach of privacy. This concept of privacy also aligns with existing data protection legislation regimes in other nations.

Meanwhile, in July 2017, the Indian government nominated Justice B.N. SRIKRISHNA as the chairperson of a group of experts on data privacy regulations in India. This committee was formed to look at the many concerns of data protection in India. On July 27, 2018, the committee submitted its full reports on laws relating to law enforcement, as well as a draught Personal Data Protection Bill. The law that was introduced in parliament was based on the report and the new bill.

Many aspects from the European Privacy Law, the General Data Protection Regulations, were incorporated into the proposed data privacy bill (GDPR). The legislation established legal foundations for the acquisition and use of personal information. In addition, the bills provide a set of rights, responsibilities, and obligations for the collecting and maintenance of personal data, as well as a DPA for regulatory and enforcement purposes. It will apply to all

¹¹Aforesaid Case: K.S. PUTTASWAMY V UNION OF INDIA taken from the INDIANKANOON.

¹² Art.21 referred from the bare act of Constitution of India.

organisations in India if it is adopted, with the exception of those that are specifically exempted. Any organisation that collects data through automated techniques would be included. It argues that data should only be gathered with free and specific consent, and that such consent should be informed with a manner that allows it to be revoked in a fair amount of time. Any data collected and received without free consent or with a malicious intent would be considered a violation, and sanctions would be imposed. It also focuses on the standards for data localisation and the employment of data protection officers in organisations. The bill establishes a strong, cross-border and sectorial framework for India's privacy and data protection.

Foreign Data Protection Legislation:

A. Regulation on Personal Data Protection (GDPR)

The General Data Protection Regulation (GDPR)¹³ is a comprehensive privacy law developed by the European Union in 2016 and implemented on May 25, 2018. It was written to replace the 1995 Data Protection Directive, which was out of date. GDPR strives to ensure that personal data is protected in a consistent manner across EU countries. GDPR's goal is to improve digital security by requiring businesses to preserve EU residents' personal data and privacy by providing them more control over the personal data they disclose online. It affects enterprises all across the world.

GDPR must be followed whenever any firm or website has the potential to collect personal information from EU citizens. The GDPR focuses on more recent issues such as privacy rights, data security, data control, and governance. The GDPR also governs personal data transfers outside of the European Union.

B. California online privacy protection Act (CALOPPA)

The California Online Privacy Protection Act (CALOPPA)¹⁴ was established to protect California residents' privacy rights and personal information. The law becomes effective on July 1, 2004. It applies to website or online service operators who collect or access personally identifiable information about California residents. If your business, website, or online services have the potential to process personal information from California citizens, it applies to another country. The "CALOPPA" requirements must then be followed by the firm in another country.

¹³ GDPR available at the digital guardian

¹⁴ CALOPPA Available at the blog of privacy policies.

This law covers commercial websites and mobile applications that access mobile and tablet devices.

C. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 is a federal statute that President Bill Clinton signed in 1996. It is implemented with the goals of ensuring that the privacy and security of patient health information is a top priority for patients, their families, hospitals, Health-Care service providers, health-care professionals, and governments. It necessitated the development of National-level Standards to safeguard sensitive Health-related information without the patient's consent or knowledge. The Health Insurance Portability and Accountability Act (HIPAA)¹⁵ applied to businesses that provide Health-Care services. It was necessary to strike a balance between maintaining the usage of personal information while safeguarding the privacy of patients seeking Health-Care and healing. HIPAA infractions can cost a health care company a lot of money in the form of Civil or Criminal penalties.

D. Personal Information Protection and Electronic Document Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to businesses in the private sector. It went into effect on April 13, 2000, with the goal of protecting customer personal information acquired by commercial companies. It also protects the consumer's personal information and gives them confidence when they share their personal information with private companies via online services and e-commerce. Before collecting, using, or disclosing any personal information, private organisations are required by PIPEDA¹⁶ to obtain consumer consent. Consumers cannot be denied services or commodities based on whether or not they consent to the collecting of their personal data.

E. Countries of Africa

There are 19 countries on the African continent that have passed data protection and privacy legislation. Data protection legislation is being drafted in six nations. The rest of the world lacks data protection and privacy legislation. In 2014, the African Union adopted the innovative Cyber Security and Personal Data Protection Convention. This convention has only ten signatures and two framers.

¹⁵ HIPAA Available at the hhs.gov.

¹⁶ PIPEDA Available at priv.gc.ca.

F. Asia and the Pacific

Data protection and privacy regulations exist in both Australia and New Zealand. In Australia, the government has revised the legislation relating to the Australia Privacy Act 1988 to meet the demands of the digital era, including mandatory reporting of any breach of personal data to the data protection authority and timely notification of impacted customers. The Privacy Act regulates how businesses acquire, use, keep, disclose, or allow access to personal data in New Zealand.

In Asia, 15 nations have data protection and privacy legislation in place, while four more are in the process of creating privacy legislation.

RECOMMENDATIONS:

1. Personal data is becoming increasingly valuable and important to businesses all around the world.
2. It is becoming increasingly vital that adequate legislation be enacted to ensure its protection. However, as the cyber world develops, anyone from any corner of the globe can access any information relating others at any moment, posing a serious threat to personal and confidential information. Globalisation transforms the entire globe into a computer system, allowing anyone to manipulate any information with a single mouse click.
3. Companies who wants do business in India but have their data controlled and transferred to another country have identified this issue as a source of worry. The government is considering the concerns of businesses and will work on enacting a data protection bill in the future that will address the country's data protection needs.

REFERENCES

Websites:

1. DME Journals of Law, Volume 1, 2020, available at <https://dmej.dme.ac.in/article/bandita-das>.
2. Dhriti, "Right to privacy in Digital age", Available at Manupatra.com, dated: Dec 27, 2022.
3. Makhija, Heena, "Analytical study on right to privacy issue and challenges in digital era", Gujarat University, INFLIBNET Centre, available at

<http://hdl.handle.net/10603/393755>.

4. Sodhganga, “Right to privacy and data protection laws in India balancing rights and managing conflicts”, available at <https://Sodhganga.inflibnet.ac.in>.

Cases:

1. K.S. Puttaswamy V Union of India
2. Kharak Singh V. State of Uttar Pradesh
3. Govind versus state of Madhya Pradesh and Others.
4. M.P. Sharma and Others VERSUS Satish Chandra

Books:

1. Right to Privacy and Internet, writer Nishant Singh.
2. Information Technology, Bare Act.



WHITE BLACK
LEGAL.