



INTERNATIONAL LAW
JOURNAL

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

Peer - Reviewed & Refereed Journal

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

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

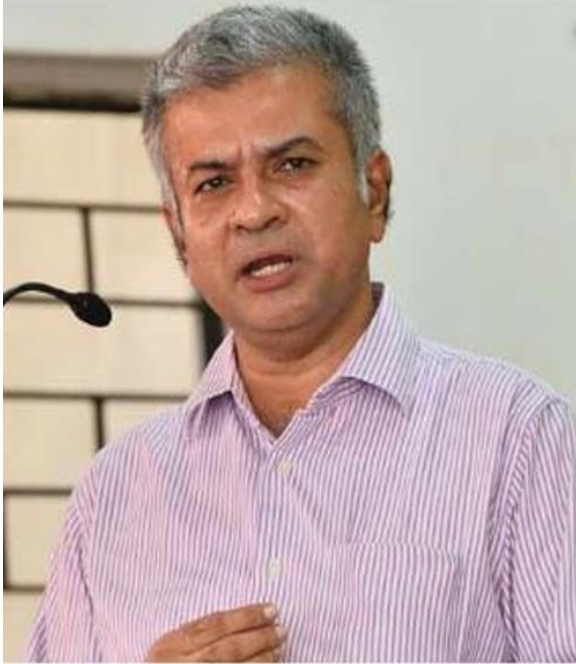
No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

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

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

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



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

professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

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



Senior Editor

Dr. Neha Mishra



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

Ms. Sumiti Ahuja

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



Dr. Navtika Singh Nautiyal

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

Dr. Rinu Saraswat



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

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

Dr. Nitesh Saraswat

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

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

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



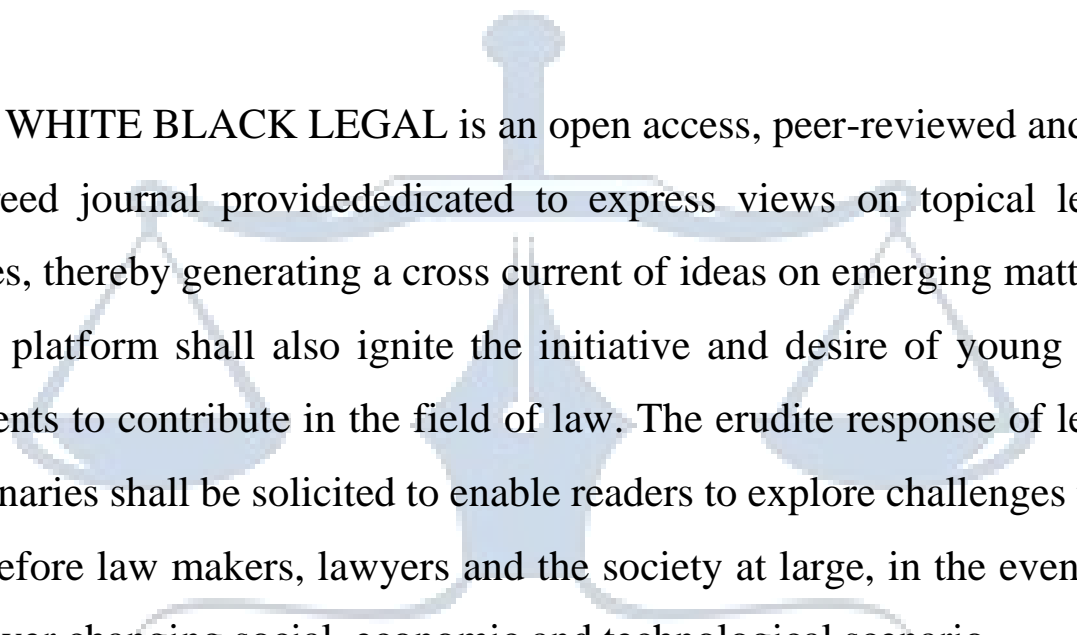
Subhrajit Chanda



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

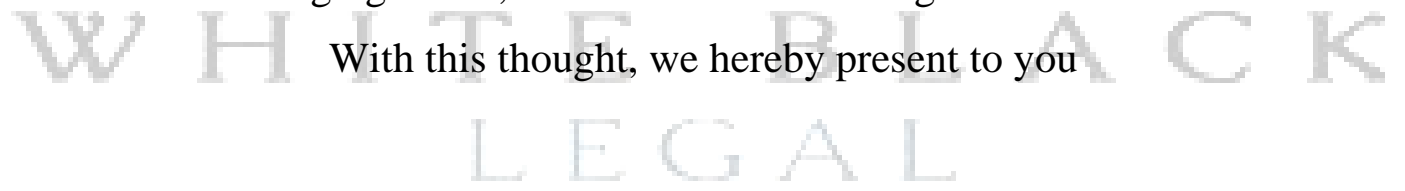
Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International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

ABOUT US



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

With this thought, we hereby present to you



RIGHT TO PRIVACY IN THE DIGITAL AGE: A CRITICAL ANALYSIS

AUTHORED BY - MANAS GULATI

ABSTRACT

My research paper focus on the impact of digital era in privacy. I have further discussed how data is important in the digital era and why we should be concerned about it. The paper also focuses on what are the laws regarding data privacy in India and how frequently they are changing. The paper also tries to explore what measures can be taken to protect privacy in the digital age

INTRODUCTION

Privacy in the simplest sense means, the right of each person to keep his affairs to himself and to determine for himself to what degree they are the subject of public observation and discussion. Privacy is about choice, choice of revealing or not disclosing, details of yourself and your life.

Every person has certain thing aspect or anything about there lives that they want to keep it to themselves to not share such thing with the world. It can be anything irrespective of whether it is serious or trivial. it's innate in us to want to take certain facts in certain details about our lives and keep them to ourselves and only release them to people that we trust people that we value and people that understand us but as we move forward in time where the ability to control that information is becoming less and less easy we have to ask ourselves how do we protect those facts how do we keep our privacy in a digital age.

Throughout mankind privacy as a concept has remain the same but privacy as a practice or an action has changed significantly. With the advancement in technology and emergence of internet privacy has certainly changed. The way we communicate, work, study has changed because of the internet. How we perform daily activities has changed. We can gather any information with a click of a button at any time. We can talk with people from all over the world on social media. Internet has made our life certainly easy but there is a price to pay for all this luxury. The price we have to pay for all this

luxury is our privacy. What a person wants to share with the world is not entirely upon him. There have been numerous cases throughout the world where data has been leaked for eg Air India data breach where Hackers gained access to Air India's database in February 2021 and took 4.5 million customers' personal data with them, CAT data breach, Upstox data leak, Police exam data spill (2019) and Cyberabad data theft (2023) As we head into an era in which we are inherently connected, via the Internet of Things, to our devices and each other, privacy will become an even more disparate and complex landscape. We need to move forward into this new age with a better understanding of how to ensure privacy rights are protected and preserved.

WHY RIGHT TO PRIVACY MATTERS

Many individuals believe that they shouldn't have to worry about their privacy on the internet if they have done nothing suspicious. This perspective on right to privacy is incomplete since it doesn't matter if you have done anything wrong or not because your information can still be used against you in way that it might harm you

Dr. Sidney Gerard, who did a lot of his privacy research back in the 60s and 70s as technology really started to come on board, wanted to study the personal aspect of it. He studied groups of people who had limited privacy rights but not just prisoners. He took people and studied them in environments where they couldn't shield facts where they couldn't present the face they wanted to present and what he found that those people had higher incidences of depression anxiety and then often times it manifested in physical pain. The important aspect of dr. Gerard's research is that invasion of privacy affects each of us individually whether we realize it or not.

WHY RIGHT TO PRIVACY HAS BECOME A BIGGER CONCERN IN THE DIGITAL AGE

It's late at night, you enter and lock the front door behind you. Doors are shut, curtains are closed and doors are locked just before you go to bed. This is what you do to protect your identity, privacy and the artifacts that make up your life.

Although our privacy at home is covered by drawn blinds, closed doors and thick walls, the digital walls covering our online lives are now much transparent. Many who sit behind these glass walls, consisting of businesses, algorithms and employees, large thousands of people, hold a constant need for our personal information, data and behaviours as it drives their business models.

Before internet there were not a lot of avenues for people to share their thoughts or ideas. We didn't have access to information from all over the world. We shared information with less people. Now can we share our data regularly over the web. Privacy before internet was a physical concept. Now with our data spread all across the world privacy has is not merely physical. We've created digital footprints which are spread all across the web. Data has become a commodity in the digital age.

HOW ARE WE SHARING PRIVATE INFORMATION IN THE DIGITAL ERA

When joining tournaments, building various profiles and connecting services out of convenience, many of us are eager to place our personal data at the feet of social media ghosts like Facebook. If it's likes, dislikes, partnerships, behavioural features or political leanings, Facebook is a gold mine for advertisers searching for data from users.

Whenever we download a new app we never bother to look at the terms and condition. We just tick the box (I have read all the terms and conditions mentioned above). You give access to these app to know your contact information, location, images. Basically you give access to most of the information present in your phone.

Uber has a mapping tool which discloses the information of its consumers who book a cab. Corporate workers have access this tool. Airbnb asked its customers to upload videos, images for verification. Facebook transmits people's names and their friends names to numerous internet tracking companies. Police forces and companies are using cameras to track license plates and build a database of points. Governments are monitoring us all over the web. Intelligence agencies are using technology to track the activities of criminals. When we open a web site a box pops up asking us to accept the cookies we never read what these cookies are. Cookies are small bits of data which are stored in a browser as text files. Websites use these tiny bits of data to track visitors and allow user-specific features. So any time you visit a web site, there is a strong chance that many different organizations will follow any move you make. They see what you're clicking on, which pages you're visiting, and where you're heading next after you've visited their page. They facilitate core website functionality, such as shopping carts for e-commerce, and are often used for more contentious reasons, such as monitoring user activities.

Governments are trying to link all of our information on a single platform. Aadhar card is the biggest

example of this.

HOW OUR PRIVATE INFORMATION CAN BE USED AGAINST US BY COMPANIES, GOVERNMENT

If a company has personal data (your interests, your political stance, what makes you happy, what makes you sad, etc.) and a means of reaching out to its audience (targeted ads, social media, etc.), then they may have a huge influence not only on individuals but society in general.

An argument is made that what's wrong with companies using data for marketing or to sell their product. The problem is the influence they can have on an individual or society with the information they possess.

The more information you have about someone, the easier it will be to trick them into believing anything you want them to believe and to lie to you. You only need to show them the part of you that you know they'll like; you no longer need to present a positive impression of yourself generally.

The digital world is monopolistic as well. Worldwide, the majority of people utilize one search engine, five social networking platforms that cater to most users, and one single shopping marketplace.

Due to their predominance in the market, this has resulted in a scenario where relatively few corporations have control over significant amounts of information.

Also the data that exist in these platforms is not entirely safe as it is prone to hacks. There have been several instances of data breach india over the last few years

Data breaches that occurred in India between 2022 and 2023 demonstrate how susceptible the country is to cyberattacks in a number of industries:

AIIMS hack. In December 2022, a hack occurred at the All India Institute of Medical Sciences (AIIMS), leading to the encryption of 1.3 gigabytes of data./

MoChhatua Breach: Sensitive user data was exposed in May 2023 due to a breach that occurred on the Odisha local governance app MoChhatua.

Zivame Data Breach: A security breach at the online women's clothing retailer Zivame exposed 1.5 million customers' personal information.

Cyberabad Police Data Leak: In April, a significant hack revealed 66.9 crore people's and organizations' data, which resulted in the apprehension of a person suspected of data theft.

Swachhta Platform Hack: In September 2022, a breach on the Swachh City platform revealed sensitive user data.

Data is used by companies for targeting ads. Targeted advertisements can be utilized to promote unhealthy meals to the fat, dubious medical procedures to the sick, and junk goods to the scientifically ignorant.

CAMBRIDGE ANALYTICA CASE

By using Facebook users' personal information to create psychological profiles, Cambridge Analytica was able to manipulate behavior and deliver precise political messaging. Through an analysis of customers' habits, likes, and other data, the company developed comprehensive profiles to forecast political views. With the use of these profiles, accurate microtargeting was made possible, enabling customized political ads to target particular demographics. By applying psychological insights to its persuasion strategies, Cambridge Analytica was able to increase their efficacy and perhaps impact users' political opinions and behavior. The controversy called into question how data privacy laws should be implemented in the digital era and brought attention to the moral dilemmas associated with using personal information for political purposes.

PRIVACY INVASION BY GOVERNMENT

In the digital era, governments hold enormous authority by gaining access to private information to provide safety and protection. After the Edward Snowden case we have learnt that government agencies have unprecedented access to our personal data. However, the scope of this power raises

basic concerns about individual privacy rights and the appropriate bounds of government authority. While governments have a responsibility to protect their populations from a variety of dangers, including terrorism, cybercrime, and public health catastrophes, the techniques used must be guided by legality, proportionality, and accountability. There has to be a balancing of individual interest and societal interest.

With fast technological advancements, governments have gained unparalleled access to people's everyday lives and activities, and this will continue. If surveillance is unregulated, particularly without clear monitoring and accountability, governments may gain too much power and potentially abuse it. This may jeopardize democratic principles and the liberties we cherish.

China's Social Credit System includes a master database, a blacklisting system, and a reward and punishment mechanism. Local and national government entities combined their data into the database and created their own lists of "good" and "bad" conduct. Those on the "good" lists are granted special advantages, whilst those on the "bad" lists have their rights limited. So yet, only local governments have established such systems, but many feel that a national program is only a matter of time.

All of this raises concerns about data security, particularly concerning personal freedom. Should governments have so broad access to personal information?

Should they be able to use and transport it anywhere they want?

Events in the past and present demonstrate that politicians and public administrations have a poor track record of exploiting intelligence against their own citizens for personal advantage. We do not need to point to India. After all, Watergate was not that long ago, and comparable situations are undoubtedly currently occurring throughout the world.

EVOLUTION OF RIGHT TO PRIVACY IN INDIA

In order to understand the evolution of privacy laws in India it is important to have knowledge about US privacy laws as Indian judiciary relied upon those for interpretation of privacy laws in India.

The American Constitution provides for certain inherent right that includes right to liberty and pursuit

of happiness and these rights should be protected by statutes, laws, rules, regulations. But privacy laws were lacking in USA.

Warren and Hardy article on right to privacy played an important role in development of right to privacy. They contended that everyone has a legal right to be left alone and control their personal information. They argued that right to privacy was implicit in common law and should be explicitly recognised

IMPORTANT CASE LAWS TO UNDERSTAND HOW RIGHT TO PRIVACY BECAME A FUNDAMENTAL RIGHT IN USA

GRISWOLD VS CONNECTICUT

In this case a state law was struck down that banned contraceptives for married couples asserting a constitutional right to privacy. The court reasoned that banning contraceptives would lead to violation of right to marital privacy

ROE VS WADE

In this case the Supreme Court affirmed a woman's right to abortion under the fourteenth amendment. The court contended that right to privacy under the fourteenth amendment extends to woman's decision to terminate her pregnancy Lawrence vs Texas

In this case the court struck down Texas anti sodomy law affirming right to privacy under the fourteenth amendment. The court contended that right to liberty includes not only physical freedom but also includes personal decisions.

IMPORTANT CASE LAWS FOR DEVELOPMENT OF RIGHT TO PRIVACY IN INDIA

The right to privacy in India has evolved significantly since the Constitution's establishment. Initially not explicitly included in basic rights, its interpretation began with court debates.

MP Sharma vs Satish Chandra 1954

In this landmark case the Supreme court dealt with legality of search and seizure under criminal law. The court held that search and seizure conducted were legal and did not violate any fundamental

rights guaranteed by Indian Constitution and also contended that search and seizure come under overriding Power of the state for protection of social security if under due process of law

Kharak Singh vs State of UP 1963

In this case certain provision of Uttar Pradesh police regulations which allowed for surveillance and domiciliary visits were challenged. Court upheld the provision as not violating any fundamental rights and did not recognise right to privacy as a fundamental right. Judge Subha Rao in his dissenting opinion argued for importance of individual privacy

Govind vs State of MP 1975

In this case held that right to privacy can only be infringed upon if there is a compelling state interest that justifies such violation.

Maneka Gandhi vs Union of India 1978

In this case a very wide interpretation was given to article 21 of Indian Constitution which played an important role in recognition of right to privacy as a fundamental right under article 21

Mr X vs Hospital Z

In this case the court determined that when there's a clash between two fundamental rights, such as the appellant's right to privacy and Ms. Akali's right to lead a healthy life, the right that advances public morality or interest takes precedence. In this case, Ms. Akali's right to know about her prospective partner's HIV(+) status was upheld as it aligned with her right to lead a healthy life under Article 21. The court ruled that disclosing the appellant's HIV(+) status did not violate confidentiality or privacy rights, as it was essential for protecting public health.

PUCL VS UNION OF INDIA 1997

In this case the court recognised that right to privacy is an inherent right under Article 21. The court held that interception of phone calls without proper procedure would violate Article 21 and Article 19(1)(a) of Indian Constitution unless it was permitted by law

R.M Malkhani vs State of Maharashtra

In this case court contended that at no point of time and individual's right to privacy can be violated except by due procedure established by law

Ram Jethmalani and Ors. vs. Union of India (UOI) and Ors The supreme court held that,
“Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner. State cannot compel citizens to reveal, or itself reveal any of their details to the public at large, either to receive benefits from the State or to facilitate investigations, and prosecutions of such individuals, unless the State itself has, through properly conducted investigations, within the four corners of constitutional permissibility”

Case Name: Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.

Facts: The case originated from a challenge to the constitutional validity of the Aadhaar project, which aimed to issue unique identification numbers to Indian residents. The petitioners contended that the project violated the right to privacy. The Attorney General cited precedents like M.P. Sharma and Kharak Singh, which suggested the absence of a fundamental right to privacy under the Indian Constitution. The case was referred to a nine-judge bench due to conflicting precedents.

Issue: Whether the right to privacy was a fundamental right under Part III of the Constitution of India.

Arguments: The respondents relied on M.P. Sharma and Kharak Singh, arguing that the Constitution did not intend to recognize privacy as a fundamental right. The petitioners contended that these judgments were based on outdated principles. They argued for a broader interpretation of privacy as a fundamental right, aligning with international human rights norms.

Decision: The nine-judge bench unanimously held that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution. It overruled the judgments in M.P. Sharma and Kharak Singh, stating that they did not fully comprehend the constitutional framework. The court emphasized that privacy is not an absolute right and may be restricted under certain circumstances, subject to legality, necessity, and proportionality. It affirmed that sexual

orientation is a fundamental aspect of privacy and recognized informational privacy as well. The court left the formulation of data protection laws to the Parliament.

Significance: This landmark judgment established the right to privacy as a fundamental right under the Indian Constitution. It provided a comprehensive framework for assessing privacy claims and emphasized the need for legislative action to protect privacy in the digital age. The case has far-reaching implications for individual liberties and government surveillance practices.

ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023, is a watershed moment in India's road toward comprehensive data privacy laws. The Act, enacted in response to rising concerns about data protection and privacy rights, seeks to build a strong framework for protecting personal data in the digital era.

At its foundation, the Act tries to strike a difficult balance between promoting innovation and respecting individuals' privacy rights. It recognizes the inherent worth of personal data and the necessity to control its collection, processing, and storage in order to prevent misuse and abuse.

One of the Act's primary aims is to create explicit criteria for the processing of personal data. It defines personal data as any information that may be used to identify an individual, such as demographic and biometric data. The Act defines numerous data processing activities, including collection, storage, sharing, and use, and underlines the need of getting explicit agreement from data subjects for such actions.

Consent is a prominent element throughout the Act, and it must meet severe conditions to be legal. Consent must be freely given, specific, informed, unconditional, and unequivocal, and persons must be informed clearly and transparently about the aim of data processing.

To guarantee compliance with the Act, data fiduciaries, or entities in charge of processing personal data, are subject to a number of requirements. These requirements include processing data solely for

legitimate reasons and with express authorization, employing security measures to ensure data integrity, and responding quickly to data breaches. Data fiduciaries must also hire a data protection officer to ensure compliance and react to data subject requests.

Despite its emphasis on individual privacy rights, the Act recognizes the usefulness of data in promoting innovation and economic prosperity. It includes rules that make it easier to process data lawfully for legitimate purposes including research, archiving, and statistical analysis. However, these measures are subject to strong restrictions designed to prevent abuse and guarantee responsibility.

Another important feature of the Act is its extraterritorial application, which extends its authority to data processing operations done outside India yet targeting Indian data subjects. This clause requires foreign firms who provide products or services to Indian people to conform with Indian data protection rules, therefore improving the protection of Indian citizens' personal data.

Despite its lofty intentions, the Act confronts several hurdles and questions about its implementation and efficacy. One source of worry is the government's wide powers, including the ability to exclude some organizations from compliance with the Act's terms. Critics contend that these features might undercut privacy safeguards and lead to possible government spying.

Furthermore, the Act's dependence on permission as the principal foundation for data processing raises concerns about its practicality and efficacy, especially in circumstances where persons do not fully comprehend the consequences of their consent or consent is gained under duress or coercion.

Additionally, the Act's enforcement methods and consequences for noncompliance have yet to be thoroughly tested. While the Act authorizes the Data Protection Board of India to investigate infractions and issue fines, its ability to hold data fiduciaries accountable remains to be seen.