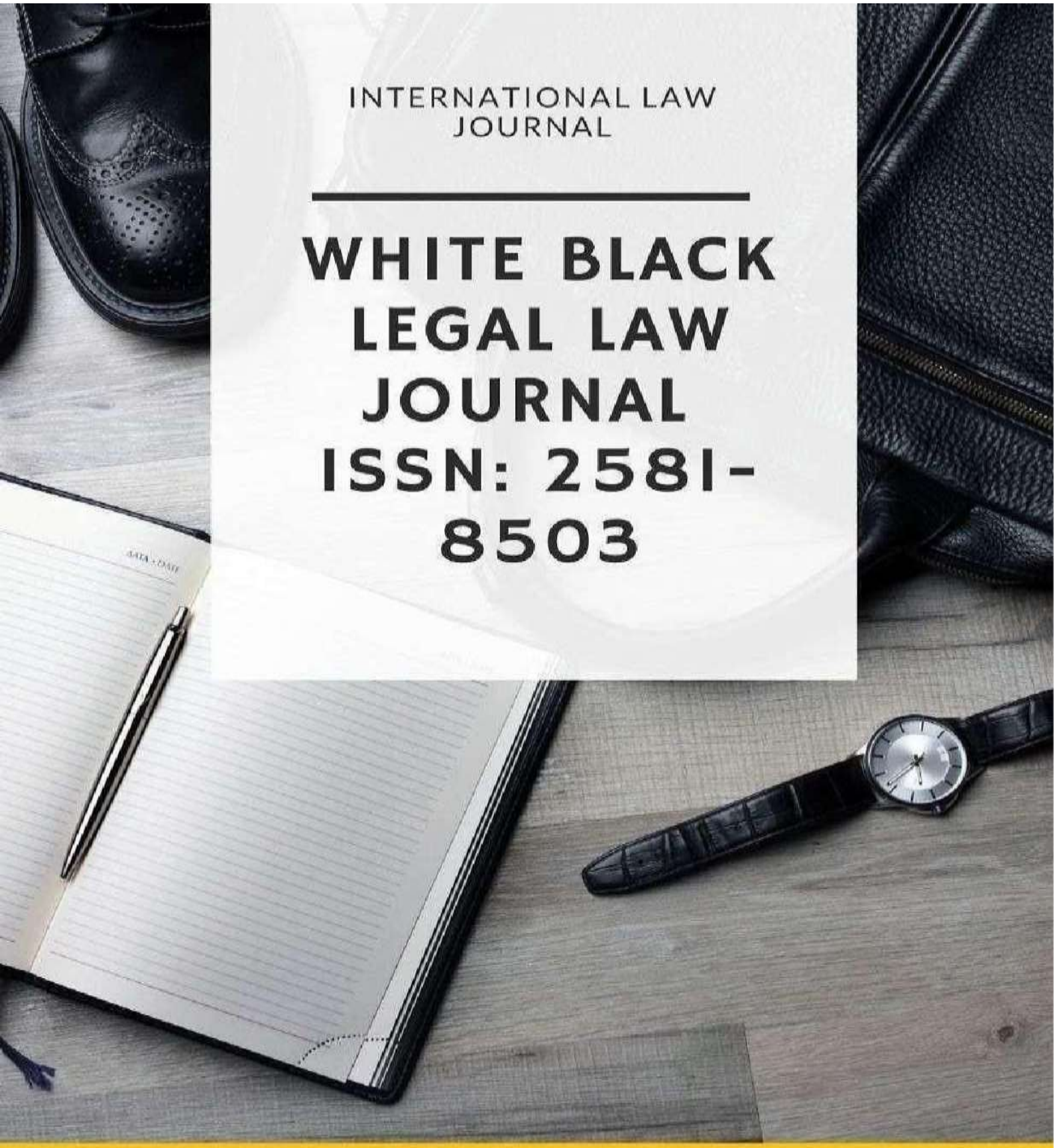

INTERNATIONAL LAW JOURNAL

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.

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.

PRIVACY AS A FUNDAMENTAL RIGHT IN THE DIGITAL AGE

AUTHORED BY - U. VISHAL CHAND CHOUDHARY & S. KALAIVANI

Abstract

Digital technology has quickly changed how we communicate and interact with the world. Digitalization has made many things faster and easier to do, but now that we collect so much data on a regular basis, there are even more issues around protecting personal information and privacy. Privacy is one of the most debated and important fundamental rights that we face today because we live in an era of mass data collection, surveillance technology, artificial intelligence, and algorithm-based government.

The recognition of privacy as a fundamental right through the case of Justice K.S. Puttaswamy v. Union of India (2017) represented a major milestone in constitutional terms as privacy was confirmed to be part of the right to life and personal liberty within Article 21 of the Constitution of India. The case changed the legal landscape by establishing that informational self-determination, dignity and autonomy are core values embedded within the Constitution of India. However, the challenges we face with privacy today have changed dramatically in the digital age, and educators, governments and business are dealing with issues such as state surveillance, commercial use of personal data, cybercrime, biometric identification and cross-border data flows as a result of the changing nature of how people relate to one another and interact with their environment in this digital age.

The goal of this research paper is to provide an overview of how privacy has changed as a core right in our society; its legal basis; and how digital technologies present new challenges for maintaining our rights to privacy. It also looks at new laws and regulations being implemented to establish an appropriate balance between privacy rights, national security interests, and advances in technology. Finally, this study will provide recommendations on how we can protect the privacy of individuals in the 21st century while still providing for democratic accountability and technological advancement.

Recognition of Privacy as a Fundamental Right

The formal recognition of privacy as a basic human right in terms of the Constitution

of India is one of the most significant changes in constitutional history in these recent years. The judicial decision provides a significant change to modern Indian constitutional law. The Supreme Court of India declared that privacy belongs to life and personal liberty (article 21) under the Constitution; and, is intrinsically linked with other freedoms identified in part III of the Constitution. This decision not only overruled previous Supreme Court decisions (M. P. Sharma (1954) and Kharak Singh (1962)), but also created a comprehensive legal framework for the protection of privacy in the digital age.

This case originated from the challenge to the constitutionality of the Aadhaar Project by petitioners who argued that requiring Aadhaar numbers of people to access public services would violate their privacy and individual autonomy by forcing them to submit to government oversight. Recognising how important the question of privacy was, the Supreme Court appointed a nine judge bench of justices (the full bench) to determine whether privacy is an enforceable constitutional right under any provision of the Constitution. The full bench unanimously declared that privacy is a constitutional right under the Constitution, and thus, overruled all previous legal authority that determined the contrary (M. P. Sharma and Kharak Singh) by holding that privacy is a right under the Constitution.

This judgment is notable not only for its outcome but for its constitutional and philosophical justifications. The court found that the constitution is a living document whose provisions need to be interpreted in light of developing social conventions. The court rejected the argument that individual privacy must be enumerated within the constitution before it could be constitutionally protected, as the court affirmed that individual fundamental rights are interdependent, and that individual privacy is an inherent condition in the protections provided by the constitution – through the guarantees of life, liberty, equality, and dignity. The court found that individual privacy was not a separate, isolated right, but rather was a prerequisite to the effective use of the other fundamental rights.

One of the primary contributions of the Puttaswamy Judgment was the Courts recognition of the many different ways in which privacy can be understood. The court recognized 3 separate dimensions of privacy: bodily privacy, decisional autonomy, and informational privacy. Bodily privacy ensures the sanctity of the human body from unwanted forced intrusions; decisional privacy protects the right to make intimate personal choices relating to marriage, reproduction, sexual orientation, and other facets of an individual's lifestyle; and informational privacy protects an individual's ability to control their personal information and provides safeguards against the unauthorized collection and use of an individual's personal information. By articulating the numerous ways individuals may

experience privacy, the court has established a clear framework for addressing challenges associated with new technological developments.

The right to privacy has a close relationship with the idea of human dignity; the Court found human dignity to be a core underlying value of the Constitution and said that privacy protects autonomy and dignity. Without privacy, a person's ability to develop themselves, build relationships, and communicate freely will be compromised by having their privacy invaded. Therefore, the right to privacy is not just a formality; it is fundamental to living in a democracy.

Also, this decision gave clear guidance on how to assess privacy violations. The three requirements needed for any breach of someone's right to privacy to be justified are (1) laws exist for the action, (2) the action is related to a legitimate government objective, and (3) the action is necessary and represents the less intrusive means of achieving that government objective. Therefore, the proportionality requirement has become an important constitutional standard when reviewing governmental actions involving surveillance, collecting data, and creating digital regulations.

This judgement had also stated that the process of `informational self-determination` will have a significant role in today`s digital age. To highlight the role of technology in daily life, the court acknowledged that the nature of a person is extended into their personal data. It also cautioned that if data is accessed by the State or Corporates without checks and balances, it could result in profiling, discrimination and erosion of autonomy. By protecting the right to informational privacy, the court has brought Indian constitutional law into alignment with global data protection norms.

Another important aspect of the judgement is its assertion that `Privacy` is not only applicable to vertical situations (i.e., against the State) but horizontal situations (i.e., private individuals to other private individuals). The court recognised that Private companies must also respect a person`s right to privacy when they collect an individual`s personal data. This is particularly important in the context of private technology companies who have a great deal of power over how individuals control their personal data.

The Puttaswamy judgement also addressed the suggestion that the right to privacy is only an elite issue and of little concern to marginalized communities. The court rejected this view and stated that all individuals (including the poor and vulnerable) should be afforded protection to their right to privacy. The court further stated that the right to control and use their personal data is fundamental to the dignity of an individual, no matter what their economic situation may be.

The acknowledgement of privacy as a basic human right had many effects on legislation

and policy reform; renewed efforts were made to develop comprehensive data protection legislation, and constitutional scrutiny over surveillance increased substantially due to the ruling's affirmation that privacy is a constitutional right and therefore a criterion against which all future legislation dealing with personal data/digital governance must be measured.

In conclusion, the recognition of privacy as a basic human right in the case of Justice K.S. Puttaswamy v. Union of India represents a defining moment in Indian constitutional law. The ruling redefined personal liberty by finding that there can be no true liberty without privacy; furthermore, it articulated a comprehensive proportionality analysis and added to the definition of privacy (to include informative) so that the Constitution could deal with the complexities of a digital world. Strengthening both individual entitlements and democratic principles such as accountability and transparency, the ruling sets forth a guideline for modern data-driven societies which enshrine the rule of law as a foundation for governance.

Privacy in the Digital Age: Emerging Dimensions

The definition of privacy has changed dramatically over time as we have moved into the digital age. Previously, concerns about protecting one's privacy generally centred on the idea of physical privacy (i.e. having your own private home), or at best, limited surveillance (i.e. when your activities or photographs would be observed). Today, because of the impact of the digital economy, technology has created a third dimension of privacy: the lack of awareness that digital activities can lead to violations of privacy and/or put one at risk.

`Today, with the digital economy and social networks, there has been a growth of privacy concerns related to the data collection and monitoring of individuals' behaviours and actions. In addition to breaches of physical privacy (i.e. individuals as being part of a network and constantly monitored and identifiable), there have also been new and increased uses of digital data for profiling, monitoring, and targeting individuals with specific information. For example, individuals generate data when they engage in any online activity (i.e. browsing, purchasing, or using a mobile application). Corporations collect this data and use it to develop behavioural profiles of individuals for the purpose of targeting advertisements and customizing content on digital platforms. The proliferation of digital platforms has created an almost continuous monitoring environment, in which the individual has little or no understanding of how their data will be processed. As a result, the knowledge asymmetry (between the data collector and the data subject) requires a critical need for transparency and informed consent.

Another factor impacting the situation is how governments monitor their citizens in the

digital age. They are utilizing digital databases, biometric identification, tracking of communications and facial recognition technology for a multitude of reasons such as securing the nation, maintaining order, and delivering welfare. These technologies are necessary and for the benefit of the state, however, they can also be misused to create a situation of mass surveillance and have a chilling effect on civil liberties. This creates risk through both individual and systemic invasion of privacy due to the existence of a centralized system designed to identify and monitor each individual's whereabouts, transactions, and communications on a massive scale.

The growing occurrence of biometric data collection has also created challenges with respect to maintaining privacy. Biometric identifiers that may be used include fingerprints, iris comparisons, facial recognition patterns, and DNA profiles, all of which are highly sensitive due to their irretrievable and core association with an individual's identity. Biometric identifiers differ from other methods of identification (e.g., passwords and identification numbers) since they cannot be altered after being compromised or destroyed. Because of the nature of digital storage of the biometric identifiers, there is a long-term risk to individuals' privacy as new technologies are developed, and/or as examples of data breaches and unauthorized access continue to be reported. Therefore, it will be crucial to provide appropriate safeguards for biometric authentication systems to sustain their use in interactive platforms in both the public and private sectors.

Artificial Intelligence opens up a new level of complexity with regard to digitally protecting privacy. When using Artificial Intelligence technologies, large amounts of personal information are analysed to predict future behaviour; determining one's creditworthiness; changing consumer preferences; and, even determining whether someone may be eligible to receive social services. The development and use of algorithms to profile individuals creates an automatic decision-making process that can profoundly affect the person's life. The lack of transparency associated with many Artificial Intelligence technologies, often called the "black box" of AI technologies, makes it difficult for individuals to know how decisions about themselves are being made. The lack of transparency poses significant challenges to traditional privacy frameworks by raising issues related to accountability and fairness of the use of personal data.

The commodification of data represents another challenge that is emerging as privacy concern to users. Personal data has a current market value in the digital economy. Various technology companies that collect user data Creates revenue via targeted advertising and partnerships with third parties. Within this new economy, privacy is be viewed as commodity

value, not as a core human value. As a result, individuals can consent to the collection of personal data without fully understanding the long-term implications of the consent they provided. The commoditisation of personal information violates the principles of informational self-determination and presents moral questions related to the exploitation of individuals.

One of the more prominent trends accompanying the level of digitisation of our society is the growth of global, borderless, data flows. Digital information can often flow across jurisdictions via the use of cloud-based storage and/or international servers. This creates difficulties when seeking to enforce national privacy laws because, within any specific country, a significant proportion of data may be subject to different jurisdictions/regulatory regimes. Also, a lack of clarity with respect to jurisdiction can create difficulties in holding someone accountable for the misuse of personal information and, in general, ensuring that an individual's personal information is afforded adequate protection. The global nature of digital communication highlights the need for international cooperation and the harmonisation of standards governing the protection of data, including the protection of personal information.

The increase in the level of digitisation of our society has also resulted in the erosion of the traditional distinctions that exist between public and private spaces. While certain activities may appear to be occurring within "public" digital forums, there may still be a reasonable expectation of privacy regarding that information. For example, social media postings, searches performed over the Internet, and sent/received messages can serve as a reflection of an individual's most intimate features, characteristics, and beliefs. Therefore, the expectation that an individual will receive privacy protection when communicating with others through the use of digital devices continues to be a topic of contention, particularly when information is shared voluntarily but later aggregated for unintended purposes. Courts continue to face the challenge of making determinations regarding an individual's reasonable expectation of privacy in the context of a digital environment.

Emerging technologies, such as IoT, create new challenges in protecting people's privacy. Smart devices, wearable health monitors, home assistants and connected appliances continuously gather real-time information about people through their use. This continuous data collection allows for detailed analytics about a user's habits, daily routine and health status. While the new capabilities resulting from these technologies increase efficiencies and do provide some level of convenience, they also greatly expand the ability to conduct surveillance within the privacy of the home and the intimate nature of an individual's life. Governments, therefore, must establish robust technical and regulatory measures to protect personal information in an IoT-enabled environment.

The understanding of the notion of "privacy" in the digital age is expanding beyond how we traditionally understand it. The concept now needs to be defined in terms of both the direct intrusions as well as the systemic risks posed by data aggregation, algorithmic profiling and predictive analytics. To adequately protect privacy in today's environment, there needs to be an implementation of proactive governance, transparency requirements, data minimization best practices and mechanisms to hold both public and private entities accountable.

To sum up, today's world has changed the privacy right into a new and very complicated constitutional issue. New elements of today's digital ages, such as the emergence of digital watching (or surveillance), biometrics (the ability to identify an individual using various physical features) and artificial intelligence (AI), the commercialization of data, and the ability of data to flow across national borders, have provided us the opportunity to progress technologically, while at the same time introducing new risks to privacy and creating potential vulnerabilities for people. To protect privacy (within this context), laws must be flexible enough to accommodate continual technological developments; we must put in place ethical frameworks to guide decision-making; and we have to remain committed through constant vigilance to ensuring that privacy continues to be interpreted as a dynamic right and as a right capable of adapting to new challenges while preserving individual freedoms and the values of democracy.

WHITE BLACK
LEGAL