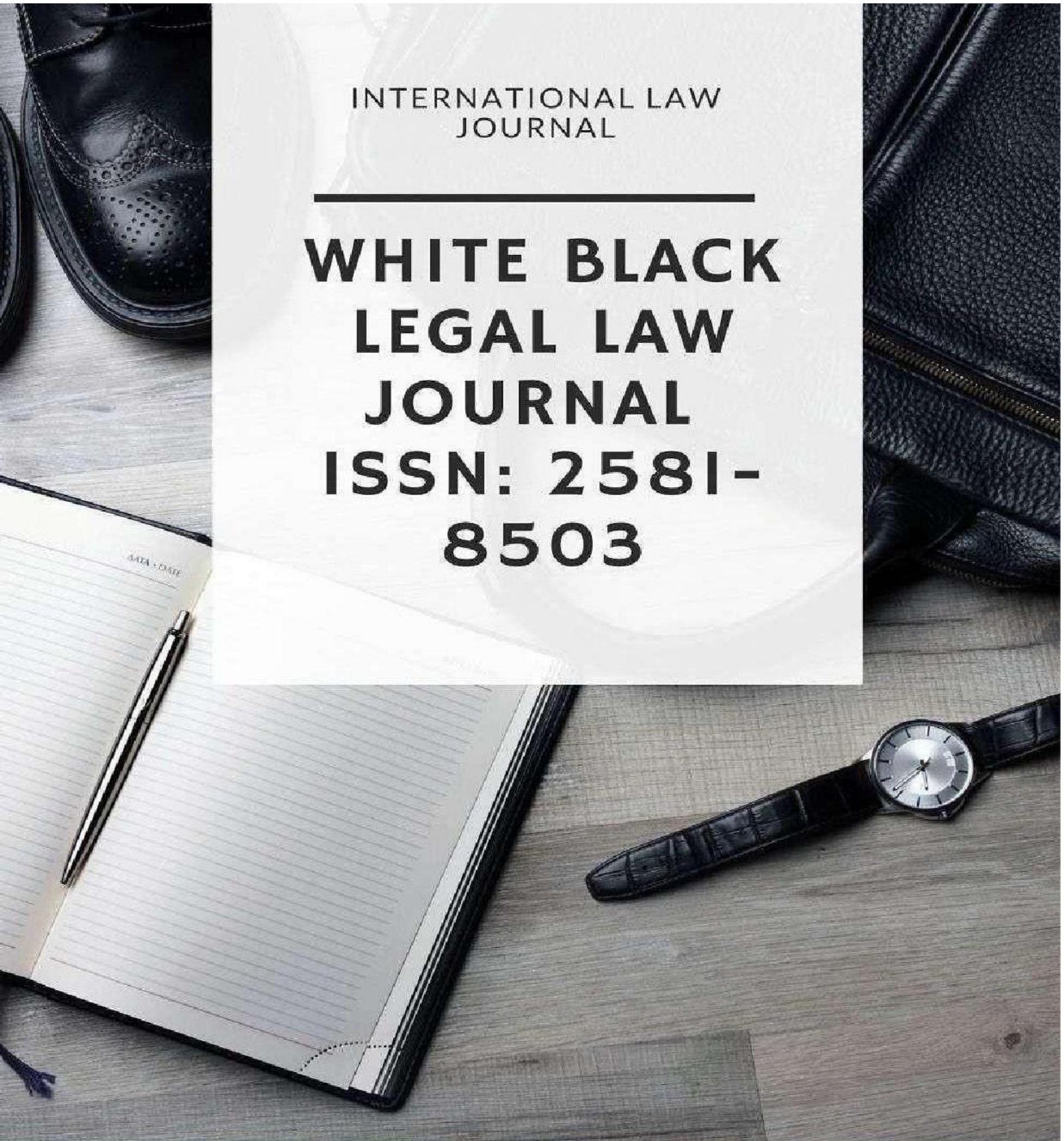




INTERNATIONAL LAW
JOURNAL

**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.

HUMAN RIGHTS IN CYBERSPACE: ROLE OF INTERNATIONAL LAW IN DIGITAL PRIVACY

AUTHORED BY - MUDITA SHARMA

ABSTRACT

In this regard, the emergence of new technologies has ushered in a paradigm shift in the manner in which human beings interact with one another, the form of governance, and economic transactions. However, the emergence of these technologies has led to greater concern over issues of privacy, surveillance, and human rights in the cyberspace realm. The subject matter under study here revolves around the problem of whether international law could help ensure digital privacy as a fundamental human right. To be more precise, the topic of interest involves examining international and non-international regimes that could regulate digital privacy, along with cases and problems of digital privacy protection in light of emerging technologies such as artificial intelligence, mass surveillance, and cross-border data transfers.

INTRODUCTION

The development of the modern digital world gives rise to different conceptions of privacy. For centuries, it meant preventing any unnecessary intrusions into an individual's home, land, and private correspondence. But the rapid growth of the internet, smartphone usage, cloud computing, artificial intelligence, and other technologies expanded the scope of the issue and now refers to the individual's digital life, data, communication, and biometric features. Nowadays, the existence of modern people is constantly registered online. Additionally, governments and private businesses collect, analyze, store, use, and even trade this data without obtaining any permission from individuals. It leads to the emergence of questions about regulating digital privacy that need to be answered.

Moreover, cyberspace does not have geographical borders. Digital information can move freely through any borders without any limitations. Consequently, it becomes challenging for a country to control its territory's digital privacy. In contrast, private businesses often have sufficient means to operate beyond any legislation's limits.

This paper seeks to determine the scope of international law in covering the issue of digital privacy. Also, it will be discussed whether there is enough legal regulation to protect human rights online.

CONCEPTUALIZING DIGITAL PRIVACY AS A HUMAN RIGHT

Privacy As a Fundamental Human Right

Human rights discourse and practice consider privacy to be one of the most important elements. It is stated in the Universal Declaration of Human Rights that nobody should suffer arbitrary interference with his privacy, family life, correspondence, and domicile.¹ This idea is supported by Article 17 of the International Covenant on Civil and Political Rights, which stipulates that States have to take measures that guarantee protection against unlawful and arbitrary actions.² However, the definition of privacy has changed considerably during recent decades. Now it also covers informational privacy, that is, the ability of a person to determine how his data will be used, collected, and shared. This idea is based on the theory of informational self-determination created by the German Federal Constitutional Court.³

Digital privacy is vital in safeguarding human dignity, autonomy, and freedom. If privacy is denied, individuals will always feel as if they are being watched, causing them to self-censor and refrain from participating in democracy. Privacy has been said to be the basis of many other rights, such as freedom of expression and freedom of association.⁴

Yet, there is no clear demarcation on what constitutes digital privacy. Digital privacy breaches cannot be easily identified compared to physical privacy infringements; moreover, digital privacy is continuous and occurs worldwide. This makes it necessary to broaden the definition of privacy under international law.

INTERNATIONAL LEGAL FRAMEWORK

Universal Instruments

International law on human rights acts as the foundation for the right to privacy. The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) constitute the key instruments addressing the right to privacy. Although both the instruments have been formulated well before the evolution of cyberspace, their flexible

¹ Universal Declaration of Human Rights art. 12, G.A. Res. 217 (III) A (Dec. 10, 1948).

² International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

³ Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 65 BVerfGE 1 (Ger.).

⁴ Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

wording makes it possible to adapt them for the cyberspace domain.

According to the Human Rights Committee, Article 17 of the ICCPR can be applied to both traditional means of communication and surveillance and data collection through digital means.⁵ The principles of legality, necessity, and proportionality must be taken into account in cases where there is an interference with the privacy of individuals.

Soft Law and UN Resolutions

In addition to binding treaties, soft law instruments play a crucial role in shaping digital privacy norms. General Comment No. 16 elaborates on the scope of privacy protection, highlighting the obligation of states to prevent both public and private interference⁶. Similarly, General Comment No. 34 connects privacy with freedom of expression, particularly in digital spaces.⁷ The United Nations General Assembly at Geneva and New York has adopted several resolutions addressing digital privacy, including the landmark Resolution 68/167 entitled “The right to privacy in the digital age”.⁸ This resolution affirms that human rights must be protected both online and offline, reflecting a growing global consensus.

New Normative Trends

Multilateral norm diplomacy involves efforts by states to devise cyber norms for states. This involves attempts by the United Nations to encourage responsible conduct by states in cyberspace. Although these are new developments, they show that the importance of digital privacy as an international issue is gradually gaining acceptance.

REGIONAL APPROCHES TO DIGITAL PRIVACY

European Union

The European Union has been at the forefront of data protection regulations around the globe due to its General Data Protection Regulation (GDPR).⁹ The GDPR provides the general principles on how personal data should be processed and introduces essential concepts such as transparency, accountability, and data minimization.

What stands out about the GDPR is that it applies even outside the jurisdiction of the European Union. This implies that organizations that are not in the jurisdiction of the European Union

⁵ Human Rights Comm., General Comment No. 16, ¶ 3, U.N. Doc. HRI/GEN/1/Rev.1 (Apr. 8, 1988).

⁶ Id.

⁷ Human Rights Comm., General Comment No. 34, ¶ 21, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

⁸ G.A. Res. 68/167, The Right to Privacy in the Digital Age (Dec. 18, 2013).

⁹ Regulation (EU) 2016/679 (General Data Protection Regulation).

may still be required to comply with the GDPR rules in cases where they process the data of individuals in the EU.

United States

In the United States, the approach to privacy legislation is based on fragmentation, using sectoral regulation for data protection like the Electronic Communications Privacy Act.¹⁰ Although the Constitution guarantees protection from unlawful search and seizure through the Fourth Amendment, its applicability in data privacy cases is limited.

This approach has been heavily criticized in academia because of its inability to address the intricacies of data privacy.¹¹

India

Significant progress has been made towards the realization of digital privacy being a fundamental right in India. The decision of Puttaswamy ruled that privacy was inseparable with Article 21 of the Indian constitution, which ensures the right to life and personal liberty.¹²

The case highlights the principle of informational privacy and emphasizes the necessity to have sufficient regulation of digital privacy. The law passed by India on this front tries to create a balance between privacy and other state interests such as national security and economic development.

CHALLENGES IN PROTECTING DIGITAL PRIVACY

Mass Surveillance

The issue of mass surveillance is enormous to digital privacy these days. It is a big deal in that governments are able to gather a lot of information about people and they themselves do not even know. This is at least partly due to what Edward Snowden divulged to the world about world-wide surveillance programs. These programs allow governments to amass vast volumes of data, intercept communications, and monitor actions of individuals on the Internet without having a particular reason to suspect an individual. The bad part of mass surveillance is that it is done in secret and there is not adequate checking by judges or transparency, so people cannot even know whether their rights are being violated or not do anything about it. This renders it difficult that people be able to defend themselves or seek assistance when they require them.

¹⁰ Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522.

¹¹ Daniel J. Solove, *Understanding Privacy* 1–10 (2008).

¹² *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

That it is all hidden and not in the open makes it even more of a challenge to contain as well. As far as international human rights law is concerned, mass surveillance poses several issues related to legality, necessity, and proportionality requirements. Surveillance measures should be provided for by a law, pursue a legitimate purpose like national security, and be necessary and proportional in pursuit of this goal. In the case of indiscriminate population-wide data collection, however, this is not possible since the rights of interest cannot be secured against everyone collectively.

In addition, mass surveillance also has a “chilling” effect on basic rights like the right to free speech and assembly. Those who know that they are being constantly surveilled may think twice before voicing their criticisms or discussing politics. This does not bode well for democracy and the strength of civil society. Thus, although governments use the justification of national security to conduct surveillance operations, there is an increasing push for tighter controls in international law.

Role of Private Corporations

Private corporations, especially large technology companies like social media websites, search engines, and big data companies, have a significant role in the contemporary digital world. They accumulate and store the information generated by individual users from their online operations. Lots of private companies make money by using people's personal data, and they do this by looking at the data to create ads that are just for them. This implies that such companies may have a reason to gather as much data as they can out of their users and in some cases this can be excessive. Humanity likes to accept the offers to provide their data without understanding what will be done with it.

The thing is that the rules regarding privacy are frequently written in such a way that it is quite hard to comprehend, and so it is difficult to make a person aware of what she/he is getting herself/himself into. That is what some experts refer to as an illusory consent - they simply think that they are making a choice, but they are not very aware of what they are choosing. And to add to the problem the information which has been collected by the private companies is sometimes shared with other parties, including the government, which can pose a significant risk should it fall into the wrong hands.

Regarding international laws, they are not exactly concerned with what big international companies are up to, but they are mostly thinking about what countries can be held responsible to. To correct this problem, the United Nations has some guidelines named the Guiding Principles on Business and Human Rights, which state that companies should respect the basic

rights of people. The thing is that these guidelines are not the laws which companies should adhere to, rather they are more like the guidelines which companies can follow in case they want to. This implies that it is the responsibility of individual companies to decide whether they will respect the human rights or not, which can be quite of a problem since not all companies can take these guidelines into consideration.

This way, there is an urgent need to have stronger mechanisms of law capable of ensuring accountability on the part of corporations. These are international laws, data protection laws, and appropriate ways of enforcing said laws. Without them, private corporations will continue to have great influence over people's personal data, thereby posing a considerable threat to privacy.

Challenges in Cross-Border Data Transfer

The international character of cyberspace means that the complex problem of jurisdiction and legal regulation arise as a result of the cross-border data transfer. Since data gathered in one country can be stored and analyzed in another country, it may get hard to tell what type of regulatory regime it is subject to. In effect, this creates a clash of legal systems of different states with different views on data protection.

Indeed, the European Union has exceptionally stringent policies regarding the protection of the data of people, with the help of the General Data Protection Regulation. However, other nations are far more lax in regards to data protection. It can be an actual issue to large businesses that conduct operations in a large number of different countries, as they will have to comply with all these various regulations. It is also difficult to make countries have control on what the foreign companies are doing within their borders.

One of the solutions to this problem may be the introduction of the data localization, which is a policy that requires some data to be localized. Nevertheless, it could also result in the adverse effect on international trade, cause costs to increase, and sharing of data to be slowed down. Such a treaty would create common criteria, set the limits of allowable monitoring, and establish enforcement mechanisms.

In addition, the inadequacy decision and standard contract clauses used by organizations across borders to protect individual information rights face similar criticism for not being sufficient enough. The lack of a unified international system leads to ambiguity and inadequate protection of individuals. This makes it necessary for organizations to improve their cooperation on an international level so as to have consistent privacy protection standards.

JURISPRUDENCE ON DIGITAL PRIVACY

The judiciary has had an immense impact on the development of concepts concerning digital privacy in the contemporary world. Indeed, courts all over the world seem to recognize the necessity to adapt existing laws to emerging technologies. With its interpretations of constitutions and application of human rights, the judiciary plays an integral part in upholding people's privacy rights.

In the case of *Big Brother Watch v. United Kingdom*, the European Court of Human Rights assessed whether bulk surveillance is consistent with legal norms, concluding that bulk surveillance should be accompanied by sufficient safeguards.¹³ In other words, it should involve independent supervision, legislative regulation, and mechanisms that allow victims of violation of privacy to seek redress.

Furthermore, in *Carpenter v. United States*, the United States Supreme Court stated that people have privacy rights as regards information related to their digital locations.¹⁴ This means that access to this type of data constitutes a search and thus requires a search warrant. As such, a reasonable expectation of privacy has been reaffirmed as a legal standard in the contemporary world.

As far as India is concerned, it is well recognized by the landmark *Puttaswamy* case that privacy is a basic right and a proportionality test must be adopted for the evaluation of any intrusion by the government. All such rulings are indicative of a realization of digital privacy as one of the basic rights that must be secured.

EMERGING TECHNOLOGIES AND PRIVACY CONCERNS

Rapid developments in technological innovations have led to some difficulties in protecting one's digital privacy rights. The emergence of such technological advancements as artificial intelligence (AI) and big data has contributed to the development of a new set of privacy-related issues since these innovations use large sets of personal data to find patterns and make predictions that can affect the decision-making processes.

Another area of concern is cybersecurity. With a growing number of attacks on digital

¹³ *Big Brother Watch v. United Kingdom*, App. No. 58170/13 (Eur. Ct. H.R. 2021).

¹⁴ *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

platforms and databases, there is a constant threat of a hacker attack or the violation of users' privacy due to a cyber incident.

Lastly, biometric technologies, including facial recognition technology and other forms of biometric identification (fingerprint scanners and iris detection software), pose a serious threat to one's privacy as they rely on collecting a unique type of data about an individual that can never be changed afterwards.

In addition, the use of surveillance technology with AI has made it possible to monitor and profile people in real time like never before. It is possible that there may be an invasive surveillance of both state and non-state entities. Given the continuous evolution of technology, current laws may find it difficult to cope. Hence, there is a pressing requirement for dynamic regulation to mitigate the risk to privacy associated with new technologies.

STRENGTHENING INTERNATIONAL LAW

In the modern context, international law should change in order to adequately address the problem of digital privacy protection. The first step that could be taken would be the creation of an international legally-binding treaty on digital privacy. One more necessary component of the solution to the problem under consideration is to strengthen the system of regulatory measures. It is also imperative to establish independent regulatory bodies and systems of judicial oversight in order to regulate the process of monitoring and safeguard the rights of individuals.

Lastly, we should consider ways of ensuring that companies are responsible of their actions. We really need rules that all countries must adhere to in order to control what companies, do, we should have rules that all countries must follow. This implies that every firm must ensure that they safeguard the privacy of individuals initially, verify how their actions will impact individuals and seek the consent of users before doing anything with their data.

The problem of harmonization of laws safeguarding privacy is also a critical one. The variations between the legal systems are likely to result in misunderstandings and poor implementation of the law. The interference of other states in the international relations, signing treaties, bilateral contracts, and the participation in the global meetings can be helpful in this case. To conclude, it is clear that the need to ensure digital privacy requires a concerted and

collective action on behalf of a myriad of different parties, including governments, international organizations, corporations, and even the civil society organizations.

CONCLUSION

Online privacy has become a significant right within the human rights in the twenty-first century. Besides transforming personal information into an asset of value, technological progress has put a large proportion of the population at high risk of being surveilled, exploited, and abused. Even though the international human rights law is a rich source of norms that are intended to protect privacy, it presents a number of challenges in adapting to new challenges. The constantly evolving environment that cyberspace creates, comprising global data transfer, dominance of personal enterprises, use of new technologies, etc. require a more innovative approach to legislation aimed at safeguarding personal information. The judicial system developments have contributed immensely to the growth of the legal protection of the privacy of the individual, but still can be improved.

To address the issues in international laws regarding privacy, we should do some few steps. To start with, we are to make international laws more powerful and improved. We should also be more collaborative with other nations and have effective systems in place to ensure that people are held accountable by what they do. By so doing, we will be making strides towards ensuring the privacy of people all over the globe.

BIBLIOGRAPHY

International Instruments

- Universal Declaration of Human Rights, G.A. Res. 217 (III) A (Dec. 10, 1948).
- International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
- G.A. Res. 68/167, The Right to Privacy in the Digital Age (Dec. 18, 2013).
- U.N. Guiding Principles on Business and Human Rights, U.N. Doc. HR/PUB/11/04 (2011).

Legislation

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
- Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522.

Case Law

- Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 65 BVerfGE 1 (Ger.).
- Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
- Big Brother Watch v. United Kingdom, App. No. 58170/13 (Eur. Ct. H.R. 2021).

Books

- Daniel J. Solove, Understanding Privacy (2008).
- Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (2014).

Journal Articles

- Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

Reports & General Comments

- Human Rights Comm., General Comment No. 16, U.N. Doc. HRI/GEN/1/Rev.1 (Apr. 8, 1988).
- Human Rights Comm., General Comment No. 34, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

WHITE BLACK
LEGAL