Page 600 - 628 **DOI:** *https://doij.org/10.10000/IJLSI.112127*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 4

2024

A Comparative Study of the Evaluation on the Right to Privacy in India and the UK, Their Legal Frameworks and Judicial Interpretation: A Cyber Law Perspective

DEV KAUR[1]

ABSTRACT

In this digital age, Right to Privacy is a fundamental right which is being acknowledge by different jurisdiction in this world. This research paper deals with a comparative study of right to privacy in India as compared with United Kingdom, concentrating their respective legal frameworks, their major judicial interpretations and examines their differences form a cyber law perspective.

The right to privacy in India is elaborated in the landmark Supreme Court judgement "Justice K.S Puttaswamy (Retd.) vs. Union of India (2017)", which declared privacy as a constitutional right under Article 21 of the Constitution of India. This landmark judgement has generated the legislative and judicial reforms that focuses on protection of personal data in cyberspace. To elaborating modern digital privacy concern, key statutes like Information Technology Act, 2000 and the Personal Data Protection Bill, 2019 are scrutinize to understand their effects and limitations.

To the contrary, the United Kingdom has a deep-rooted privacy law, named as Human Rights Act, 1998 and further reinforce by the General Data Protection Regulation (GDPR) post-Brexit through the Data Protection Act, 2018. The U. K's privacy framework is elaborated by rigorous data protection standards and strong enforcement mechanisms, considers its commitment to validate privacy rights.

This research paper examines the judicial interpretations and legislative measures of both the countries, that elaborates their strengths and weaknesses. It also defines how cultural, historical and political contexts impacts these legal landscapes. Under this paper the comparative analysis, focuses on to provides understanding of the effectiveness of the privacy protection in this digital age. Giving suggestion and recommendations towards synchronizing cyber laws at global level, also to elaborate the challenges raised by rapid technological advancements.

Keywords*: Right to Privacy, Cyber Law, Data Protection, Legal Frameworks, Judicial Interpretation.*

[1] Author is a Research Scholar at Faculty of Law, Dr. Bhim Rao Ambedkar University, Agra, India.

 [ISSN 2581-9453]

I. INTRODUCTION

Right to privacy, in this digital age has arising as a most important affair for the individuals and government alike. The excessive growth of digital technologies has given an easy way towards unparalleled data collection, their storage and its analysis give major challenges towards the safeguarding of personal privacy. This research paper focuses and examines the evolution, legal frameworks and judicial interpretations of the right to privacy in both the countries i.e. India and United Kingdom through a cyber law perspective.

(A) Background

It is globally recognized that, right to privacy is a fundamental human right. The right is enhanced in different international human rights instruments, like Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). These instruments are very necessary for protection of personal privacy against the arbitrary interference.

The concept of privacy in India has go through with major progress. Historically, the concept of privacy was not expressly written in the Indian Constitution. Although, as the year passes, our Indian judiciary has recognized and explained this right with the help of landmark judgments. The most valuable and notable landmark judgment is Justice K.S Puttaswamy (Retd.) vs. Union of India (2017)[2], which declares the right to privacy as a fundamental right under article 21 of the Indian Constitution.

As well as, the United Kingdom has also a well-established legal framework against privacy protection. The European Convention on Human Rights (ECHR) which is consolidated by, The Human Rights Act, 1998[3] provides a strict foundation for privacy rights.

(B) Objectives

The research paper wants to achieve the following objectives:

1. Analysis the legal frameworks relating to right to privacy in India and U.K: This analysis includes an examination of statutory provisions, regulatory mechanism and recent legislative developments.

2. Differentiation of judicial interpretations relating to privacy rights: By scrutinize landmark court judgments, this paper focuses to understand that, how the courts of both countries have elaborated the right to privacy.

[2] AIR (2017) 10 SCC 1.
[3] Human Rights Act, 1998.

 [ISSN 2581-9453]

3. Evaluate the efficacy of privacy safeguarding measures: This method includes to assess the practical implications of legal and judicial measures towards protection of privacy in this digital age.

4. Recognizing the gaps and suggests the improvements: According to the qualified analysis, this research paper deals with areas, where privacy laws and their enforcement mechanism can be increased.

(C) Methodology

This research paper focuses on comparative legal analysis approach, which pointing on both primary and secondary legal sources. Legal statutes, regulations and judicial interpretation from India and the UK are covered under the primary sources. Scholarly articles, legal commentaries and the reports from the relevant organizations are included in the secondary sources. The paper will firmly analyse these sources to make differences and take a perception to the effectiveness of privacy protections under both the jurisdictions.

(D) Significance

The importance of this research paper lies in its possibilities to commit to the global discourse on privacy rights. This paper is very helpful and offers valuable lessons towards policymakers, legal practitioners and research scholars, through comparing the legal frameworks and judicial interpretations between both the major democracies. However, in this digital era, where cyber-attacks and data breaches are increasingly very fast, it is very important to examine and improving privacy protections.

With the help of this comprehensive analysis, this study focuses towards understanding of privacy rights and how to safeguard them in this digital age.

(E) Book Reviews

A customary academic research paper usually does not include book reviews, analysis of important literature leads to provide context, depth and broader perspectives on the subject matter. The following reviews discusses about important books that elaborates privacy rights their legal frameworks and judicial interpretations in India and UK, majorly form a cyber law perspective. This book review helps towards the large discourse on privacy laws and elaborate the continuing developments in this field.

1. Cofone, Ignacio. (2023) There is nothing as invasion of privacy from the side of the tech firms. Businesses are able to do this because our legal system subscribes to archaic doxastic principles that cause legislators, regulators, and even judges to make erroneous assumptions

about privacy resulting in inadequate legal redress for one of the most crucial problems of the modern world. Cofone Ignacio explains myths about data-based interactions, which continue later, and gives current legislation and ideas for reform on the basis of behavioural science, sociology, and economics. Thus, the readers will have an understanding of why the existing rules and regulations cannot protect society from the detrimental impacts of corporate digital harms, especially those originating from artificial intelligence. Then, in response, Cofone suggests a better course of action: real liability for the consequences of corporate data undertakings which in the long run entails the creation of another form of responsibility that honours privacy.[4]

2. Solove, Daniel J and Schwartz, Paul M. (2023) The GDPR, Carpenter, state laws concerning biometric data, the CCPA, and many other recent developments are incorporated in the latest edition, the Seventh Edition, of Information Privacy Law. Information Privacy Law stands out as a well-organized and practically-oriented guide to the modern phenomenon of information privacy law. It contains many of the latest cases and materials concerning concepts more and materials involving emerging technology and information privacy The source also has vast background information and authors' notes that afford brief but comprehensive overviews of a range of legal considerations. comprehensive treatment of many subject matters, such as to standing in privacy cases, enforcement of HIPAA & HHS, and FTC privacy enforcement. portions of the site specifically dedicated to the privacy in workplace, school and employment, national security, and data privacy. Chapters on the government spying on its innocent citizens and freedom to try out concepts that can shape one's life. Timely reporting on Snowden, NSA, and subsequent legislation and/or regulation. an exciting way to engage with laws such as the CCPA, GDPR, ECPA, FCRA & HIPAA with game-based learning.[5]

3. Citron, Danielle Keats. (2022) The Fight for Privacy is a brand new and invigorating analysis of the concept of privacy in the twenty-first century, and instead of concentrating on the digital moguls and their exploits, it looks at the accumulative cost that falls on the user of the various platforms and apps that end up encroaching on our friendships, familial bonds, intimate connections, children, as well as one's sense of self.[6]

4. Richards, Neil. (2021) Everyone knows Companies and governments are spying on us

[4] Cofone, Ignacio. The privacy fallacy: harm and power in the information economy. Cambridge University Press, 2023.
[5] Solove, Daniel J., and Paul M. Schwartz. Information privacy law. Aspen Publishing, 2020.
[6] Citron, Danielle Keats. The fight for privacy: Protecting dignity, identity, and love in the digital age. WW Norton & Company, 2022.

they're listening to all that we are saying in the cars, in restaurants, in phone calls and anything that has a microphone -They are seeking information about ourselves and everyone we know. Various kinds of ad networks follow us while browsing the internet and serve us with 'more relevant' ads. We are now spying on ourselves and we undergo conversation surveillance with a focus on the indications of radicalism by NSA. To reduce school shootings, such schools also supervise children's Emails. Giant drones fly in the skies and cameras follow even each corner of the city and each traffic light. For the purposes of 'teaching' the artificial intelligence computers that are meant to predict anything ranging from traffic to the location of illegitimate aliens, databases inclusive of human details are created. Some of us are even quantifying ourselves with Fitbits, Apple watches and other forms of personal electronics; thus, the much talked about 'quantified self'. A recent epitome of such sentiments was heard from Mark Zuckerberg of Facebook who said, 'the Age of Privacy is over. 'Those people such as Zuckerberg who asserted loudly that 'privacy is dead' are wrong. Critic Neil Richards noted in his book, Why Privacy Matters, that privacy is not defunct but ambiguous.[7]

5. Trzaskowski, Jan. (2021) The book demonstrates how human dignity, privacy, and anti-discrimination claims could enhance these legal fields and explains how the data protection law and the marketing law are related. There is an assertion to the effect that 'paying with personal data' is actually a misleading notion because what is in fact given is attention and agency, which are worth more, which are held in higher regard and which are more scarce than personal data and are crucial for understanding sociocultural processes. This paper on why information does not lead to transparency-a state that empowers the user-develops a three-level model of information failure that explains this phenomenon.[8]

6. Sharma, Sanjay. (2019) The handbook written by Sanjay Sharma, provides a practical understanding towards the GDPR and its suggestion regarding data privacy. The book describes about the principles of data protection, rights regarding data subjects and the compliance requirement in relation with an organization.

The handbook is very important towards understanding the regulatory environment in the UK post-GDPR and also gives a detailed analysis of the legal principles that govern data protection. The practical theory and explanations of this handbook makes an important resource for legal practioners, policymakers and research scholars. The handbook contains case studies and real-world examples that elaborates the application of GDPR. This book does not exclusively cover

[7] Richards, Neil. Why privacy matters. Oxford University Press, 2022.
[8] Trzaskowski, Jan. "Your privacy is important to us." Restoring Human Dignity in Data-Driven Marketing (2021).

the broader concept of historical and judicial under the context of privacy law in the UK while focusing on GDPR.[9]

7. Westin, Alan F. (1968) Privacy is defined as a person's right to decide on the conditions under which information about him or her is communicated to others, and while there are many books published on privacy, many scholars regard Alan Westin's Privacy and Freedom, published in 1967 as the starting point of most modern discourses on privacy as it refers to technology and human liberty.[10]

8. Hartzog, Woodrow. (2018) The customers of the Internet expose oneself to technologies designed to violate any granted privacy on a daily base. This feature is applied in Internet of Things, social networking apps, and surveillance technology owing to the fact that it is hard to protect personal data. Besides, the law allows this because it is up to the users to protect themselves particularly where circumstances have been manufactured to create room for exploitation.

Nevertheless, Woodrow Hartzog disagrees with this state of affairs in Privacy's Blueprint; asserting that hardware and software developers should be compelled to the law to incorporate privacy into product design. Technology is still infused as if it is a valueless commodity by the current legal regime, with the user as the only one making the distinction of Technology working well or poorly. However, this is untrue. To Hartzog, many of the applied digital technologies' primary goal is to make people reveal information about themselves and to expose oneself.[11]

9. Richardson Megan. (2017) This book of Megan Richardson identifies the historical development regarding the right to privacy, its origin and how it has evolved over the time. The book elaborates the essential historical context which is very important for understanding the contemporary privacy rights.

This book is mainly essential for understanding the historical and philosophical aspects of privacy rights, which is very relevant for comparative legal research. The historical analysis of this book elaborates the rise of privacy rights and provides a foundational context relating to current legal frameworks of both India and the UK.[12]

10. Friedewald, Michael et al. (2017) The book analyses the balance between surveillance,

[9] Sharma, Sanjay. Data privacy and GDPR handbook. John Wiley & Sons, 2019.
[10] Westin, Alan F. "Privacy and freedom." Washington and Lee Law Review 25.1 (1968): 166.
[11] Hartzog, Woodrow. Privacy Õs Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press, 2018.
[12] Richardson, M. The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea. Cambridge University Press. 2017.

privacy and other security from citizen's perspective. This book is based on empirical research based on public attitudes in respect of surveillance and privacy through various countries. The book describes the public attitudes, which provides a valuable context for describing societal perspectives related to privacy and surveillance, which is very essential for effective legal frameworks. The book's empirical data and cross-country differences describes how different societies use privacy and with security, which provides a better context relating to legal analysis in this research paper. The main concentration of this book is on the public attitudes, which is not directly related with legal and judicial aspects of privacy rights.[13]

11. Duggal Pavan. (2014) This book is mainly focuses on the legal aspects of cyber laws is India, that includes privacy, data protection and regulatory environment. It elaborates an introduction of key legislations and judicial decisions that cover cyber laws in India.

This book is very essential towards this research paper, because it provides a detail analysis of Indian legal frameworks in respect to privacy and cyber laws. The writer's expertise and exhaustive coverage regarding Indian cyber laws, including judicial interpretations and legislative framework convert this into a valuable resource from knowing the privacy rights in India. This book is only focuses on Indian legal framework that means not related with other jurisdictions, which is very important for the holistic comparative analysis.[14]

12. Wright, David and Hert, Paul De. (2012) Under this book which is written by David Wright and Paul De Hert's, provides a deep examination of privacy and data protection under the head of modern information technologies. In this book the author analysis the impact of technologies like big data, AI and IoT on privacy, also discuss about both regulatory challenges and potential solutions. The said book is very relevant for the comparative study in the privacy laws, as it gives a comprehensive overview of the problems under the emerging technologies under privacy rights. It focuses towards the need for rigorous legal frameworks to explain these issues. This book majorly describes about detailed examination of different technological impacts related to privacy and its comparative approach, which includes the viewpoint form different jurisdictions, that includes the EU, which effects the UK law. This book majorly concentrates on European and North American context, that limits the direct applicability towards Indian legal framework.[15]

[13] Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R., & Peissl, W. (Eds.). Surveillance, Privacy, and Security: Citizens' Perspectives. Routledge. 2017.
[14] Duggal, P. Cyber Law: The Indian Perspective. Saakshar Law Publications. 2014.
[15] Wright, D., & De Hert, P. (Eds.). Privacy and Data Protection: Challenges of Modern Information Technologies. Springer. 2012.

II. LEGAL FRAMEWORKS IN INDIA

The legal framework that elaborates the right to privacy in India has emerge considerably, mainly in context of increasing the difficulties in this digital age. This area defines the statutory provisions, landmark judgements and regulatory mechanisms that all describes the privacy rights in India.

(A) Constitutional Provisions and Judicial Interpretations:

Under the original text of the Indian Constitution, it does not expressly describe the right to privacy. Although, as the time passes the Indian judiciary has played a main role in defining and acknowledging this right. The landmark case of Justice K.S. Puttaswamy also known as Aadhar case have a pivotal role to recognize privacy. In this case, Hon'ble Supreme Court of India held that, Right to Privacy is a fundamental right inherent to the right to life and personal liberty that is govern under article 21 of the Indian Constitution.

The ruling of right to privacy is emerge which is also based on earlier decisions, where the court also direct towards the existence of right to privacy. In the case of Gobind vs. State of Madhya Pradesh (1975)[16], the court held that, right to privacy is governed under articles 19 and 21. Comparably in the case of R. Rajagopal vs. State of Tamil Nadu (1994)[17], the court held that, right to privacy is impliedly in the right to life and liberty.

(B) Statutory Provisions

1. Information Technology Act, 2000[18]

The Information Technology Act, 2000 (IT Act) is the main statute that governs the digital privacy in India. Sec. 43A of the said Act mandatory gives direction to companies which is handling sensitive private data should exercise reasonable security practices and procedures for safeguarding such data. If the negligence occurs from the company side, that leads to wrongful gain or loss, the company held be liable to pay compensation.

Section 72A of the Act gives penalty to any person who, while giving services under the lawful contract, without the person's consent, discloses his personal information, with the intention to cause wrongful gain or loss.

2. Indian Penal Code, 1860[19]

The Indian Penal Code, 1860 (IPC) also have the provisions which indirectly linked with right

[16] AIR (1975) 2 SCC 148.
[17] AIR (1994) 6 SCC 632.
[18] (Act 21 of 2000).
[19] (Act 45 of 1860).

to privacy. Sec. 354C, deals with voyeurism, that means an act of watching or capturing the image of a woman engage in her private act, without any consent for that woman.

III. REGULATORY MECHANISMS

1. Data Protection Regime

To establish a comprehensive data protection regime in India, the Digital Personal Data Protection Act, 2023[20] (DPDP ACT) came into force. This bill launches several key principles, including data minimization, purpose limitation and accountability. In this act there is an establishment of an authority named "Data Protection Authority" (DPA) to monitor data processing activities and enforce compliance with law.

This DPDP act[21] classify data into three categories: 1. Personal Data 2. Sensitive Personal Data 3. Critical Personal Data, with different levels of protection in different categories. The Sensitive personal data means and includes, data related to health, sexual orientation, biometrics genetics and financial data among others. The act also has some individual's rights, like right to access, correction and erasure of personal data.

2. Aadhaar Act, 2016[22]

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 control the collection and use of biometric and demographic data through the Unique Identification Authority of India (UIDAI). In the landmark judgement of Justice K.S. Puttaswamy vs. Union of India[23], 2018, the Hon'ble Supreme Court of India upheld the validity of the Aadhaar scheme but also imposed strict conditions to protect individual's privacy.

(A) Sector-Specific Regulations

In India there are also many sectors which additionally have privacy regulations. For instance, Reserve Bank of India (RBI) has given guidelines for all banks to maintain the security and confidentiality of customer's sensitive data. As well as, the Insurance Regulatory and Development Authority of India (IRDAI) mandatorily gives instruction to insurers to adopt data protection measures.

(B) Challenges and Criticisms

In spite of these legal provisions, India's privacy legislation may face different challenges. The data protection laws and their enforcement remains weak, and there is more concern about the

[20] (Act 22 of 2023).
[21] Ibid.
[22] (Act 18 of 2016).
[23] AIR (2018) 1 SCC 809.

importance to protect against state surveillance. The enactment of Personal Data Protection Act was delayed that leads to make criticism from privacy lawyers and stakeholders.

IV. JUDICIAL INTERPRETATION

The judicial interpretation or judicial decisions regarding right to privacy in India and the United Kingdom has a very essential role towards privacy protection in both the countries. In this section it involves landmark judicial decisions and their suggestion regarding right to privacy form a cyber law perspective.

(A) India

In India the right to privacy has evolve through judicial decisions announced by the Hon'ble Supreme Court of India and other courts, which has a very main role regarding right to privacy.

1. Kharak Singh v. State of Uttar Pradesh[24]

Kharak Singh vs. State of Uttar Pradesh was one of the earliest cases that defines the concept of privacy. In this case the Supreme Court deals with the concern of police surveillance and its suggestions for personal liberty. While addressing the case, the court did not expressly identify the right to privacy, Justice Subba Rao, in his opposing opinion, deals with the existence of a privacy right, said that "nothing is more injurious to a man's physical happiness and health than a pre-planned interference with his privacy".

2. Gobind v. State of Madhya Pradesh[25]

This case established an essential step towards identifying privacy rights. The Supreme Court of India held that the right to privacy is impliedly included in the right to life and personal liberty under article 21 of the Indian Constitution. The court also held that, privacy rights have their own restrictions, but any violation by a compelling state for his interest, should be justified.

3. R. Rajagopal v. State of Tamil Nadu[26]

This case which is also known as the "Auto Shankar" Case, the Supreme Court expressly acknowledge the right to privacy, especially through the context of illegal publication of a crucial personal information. The court also held that, the right to privacy is impliedly under article 21 and extends towards right to be left alone and to protection of personal information from public scrutiny.

[24] AIR 1963 SC 1295.
[25] (1975) 2 SCC 148.
[26] (1994) 6 SCC 632.

4. People's Union for Civil Liberties (PUCL) v. Union of India[27]

This case mainly targets to the telephone tapping by the government. The Supreme Court held that illegally telephone tapping is the violation of right to privacy under article 21 of the Constitution and also laid down some guidelines to manage and restrict such practices.

5. Justice K.S. Puttaswamy (Retd.) v. Union of India[28]

The landmark case of justice K.S. Puttaswamy vs. Union of India which is also known as the "Right to Privacy case" is a milestone moment in the history of Indian judiciary related to privacy rights. In this case, a nine-judge constitutional bench of Supreme Court held that, the right to privacy is a fundamental right governed under article 21 of the constitution. The bench held that, privacy is inherent towards life and liberty and gives personal autonomy, bodily integrity and informational privacy. This judgement essential for subsequent privacy related legislations and judicial interpretations.

6. Aadhaar Judgment (2018)[29]

In the landmark case of K.S. Puttaswamy vs. Union of India which is also known as Aadhar case, the Apex Court upheld the constitutional validity of Aadhar scheme, but also imposed rigorous conditions to safeguard individuals' privacy. The court also held that, collection of biometric data for Aadhar shall be co-exist with strict safeguarding measures to anticipate the misuse and illegal access.

(B) United Kingdom

In United Kingdom, the concept of right to privacy is essentially derived from the European Convention on Human Rights (ECHR) and further strengthen through country's legislation and judicial interpretations.

1. Malone v. Metropolitan Police Commissioner[30]

In this case, the police commissioner focuses on the absence of statutory legal protection for the privacy in the UK at that time. The European Court of Human Rights (ECHR) establish that the, UK had violated Article 8 of the ECHR, which provides the right to respect for private and family life, home and correspondence, because of the absence of legal protection against arbitrary interference by the state.

[27] (1997) 1 SCC 301.
[28] AIR (2017) 10 SCC 1.
[29] AIR (2018) 1 SCC 809.
[30] [1979] Ch 344.

2. Campbell v. MGN Ltd (2004)[31]

The House of Lords, in the landmark case of Campbell vs. MGN Ltd. elaborates a cause of action for breach of confidence which is based on illegal publication of personal information. This case is very essential for the significant development of privacy law in the UK, recognizing that the individuals have logical expectation of privacy, that is related to certain personal information, and any such publication regarding such information is justified and rational by a public interest.

3. Von Hannover v. Germany[32]

This European case of Von Hannover vs. Germany had a very important role under privacy law in UK. It was held that, Article 8 of the ECHR expand to protection against intrusive media coverage, even also for public figures unless there is a legitimate public interest.

4. R (Wood) v. Commissioner of Police for the Metropolis[33]

The court of Appeal, in this case of R(Wood) vs. Commissioner of Police for the Metropolis, explains the issue of surveillance and data retention by the police officials. The court also held that, the retaining of photographs by police of a peaceful protestor breaches his right to privacy under article 8 of the ECHR, highlights the proportionality and necessity under such practices.

5. Google Inc. v. Vidal-Hall[34]

This case deals with misuse of sensitive personal data by a private organization. The court of appeal explains the right to compensation for suffer, which is caused by breach of data protection principles, without having any pecuniary loss, and also to strength the privacy rights in the subject matter of data protection.

6. Big Brother Watch and Others v. United Kingdom[35]

In this recent case of Big Brother Watch and others vs. United Kingdom, the ECHR recognized that, the UK's mass surveillance regime violated article 8 of the ECHR because of the absence of essentials safeguards and oversight mechanisms. This decision makes a balance between national security interests with individual privacy rights.

(C) Comparative Analysis:

In India and UK, the judicial interpretations of privacy rights have both similarities and

[31] [2004] UKHL 22.
[32] (2004) 40 EHRR 1.
[33] [2009] EWCA Civ 414.
[34] [2015] EWCA Civ 311.
[35] App Nos 58170/13, 62322/14, 24960/15 (2021).

differences. In India, the judiciary has increasingly expanded the scope of privacy rights with the help of landmark decisions, which gives recognition to privacy as a fundamental right. In UK, it was affected by the ECHR, which developed a rigorous legal framework related to protection of privacy through the combination of domestic and European judicial interpretations.

Both of the jurisdictions focused on the need for proportionality and necessity while any invasion into the privacy, through the state or private entities. Although, the structure of the UK is being elaborated by a more structured and comprehensive legal framework, especially with the help of GDPR and the Human Rights Act, 1998[36].

V. LEGAL FRAMEWORKS IN THE UNITED KINGDOM

In this digital era, the United Kingdom has incorporated an exhaustive legal framework for safeguarding the privacy rights. This legal framework is hold by domestic legislation, European union regulations and international human rights convention. This segment analysis the key legal instruments and regulatory mechanism that control the right to privacy in UK.

(A) European Convention on Human Rights (ECHR)[37] and Human Rights Act, 1998[38]

In United Kingdom, the right to privacy is crucially controlled by the European Convention on Human Rights (ECHR), mainly article 8, which undertakes the right to respect for private and family life, home and correspondence. The ECHR incorporated by, The Human Rights Act, 1998, that permits the individuals to approach the domestic courts in case of violation of their privacy rights.

Article 8 of the ECHR is not exhaustive and allows for intrusion by public authorities if it is lawful, necessary and ready to achieve a legitimate goal like, national security, public safety or the mitigating of crime. The Human Rights Act, 1998, includes all public bodies included court also, to act in obedience with the ECHR, thereby included privacy rights in the UK legal framework.

(B) Data Protection Act, 2018[39] and General Data Protection Regulation (GDPR)[40]

In this digital era, the most important legal structure that elaborates privacy is the Data Protection Act, 2018. Through this DP Act, the General Data Protection Regulation (GDPR)

[36] Supra note 2 at 3.
[37] European Convention on Human Rights, 1950, Article 8.
[38] Ibid
[39] No.7 of 2018.
[40] (EU) 2016/679.

implements into the UK legal framework, that ensures the protection of data standards post-Brexit. The GDPR came into force on May 2018, is as exhaustive instrument that gives strict guidelines for the processing of personal data.

a. Key Principles of GDPR

Some fundamental principles that elaborated by GDPR relating to processing of data are as follows:

Lawfulness, Fairness, and Transparency: Sensitive personal data should be refined lawfully, fairly, and in a transparent manner.

Purpose Limitation: The data collected should be for specified, explicit and legitimate purposes and not to be again processed in that matter which is incompatible with these purposes.

Data Minimization: That data should be collected and processed only for which matter, which is necessary for the intended purpose only.

Accuracy: The data which is personal should be exact and kept up to date.

Storage Limitation: Data should be in retention in a form which is related with identification of individuals only for that necessary time period.

Integrity and Confidentiality: sensitive personal data shall be processed in that way, it ensures relevant security, that includes protection of data against illegal or unlawful processing and accidental loss.

b. Rights of Data Subjects

GDPR grants individuals (data subjects) multiple rights, that includes:

Right to Access: This right is related to access the personal data and take information regarding the way their data is being processed.

Right to Rectification: Individuals have the right, to make request relating the correction of incorrect or incomplete data.

Right to Erasure (Right to be Forgotten): In some of the cases individuals have the right towards deletion of their personal data.

Right to Restrict Processing: Individuals have the right, to restrict the processing of their personal data under some circumstances.

Right to Data Portability: Individuals may request to receive their personal data in a well-structured way, usually used format and then transfer it to another controller.

 [ISSN 2581-9453]

Right to Object: Individuals have the right to object the processing of their personal data for some purposes, like direct marketing.

c. Regulatory Authority

In United Kingdom, the Information commissioner's office (ICO) is an independent authority that is responsible for the execution of data protection laws. ICO have the power to investigate into the matter of data breaches, issues fines, and make sure compliance with Data Protection Act, 2018[41] and GDPR.

(C) Investigatory Powers Act, 2016[42]

This Act is also known as "Snooper's Charter", that regulates the monitoring activities of public authorities. The Act gives a legal framework relating to interception of communication, collection of bulk data and interference of equipment's by intelligence agencies and law enforcement bodies.

a. Key Provisions

Targeted Interception and Equipment Interference: Allows targeted interdicting of communications and equipment's which interfere with proper authorization.

Bulk Powers: Allows the collection of bulk communication data and the accession of bulk personal database.

Judicial Oversight: It establishes the system of judicial commissioners who supervise the authorization of warrants in case of surveillance activities.

Data Retention: It allows the communication service providers to retain the personal data for maximum 12 months.

(D) Privacy and Electronic Communications Regulations (PECR), 2003[43]

The Privacy and Electronic Communications Regulations (PECR), 2003 supplement the Data Protection Act and GDPR through specifically elaborating privacy issues that is related to electronic communications.

Marketing: Manage unrequested marketing communications through emails, texts and phones.

Cookies: Enables the websites to obtain the individuals consent before applying cookies or

[41] Supra note 2 at 16.
[42] Investigatory Powers Act, 2016 (c.25).
[43] No. 535 of 2003

similar tracking methods on their devices.

Confidentiality of Communications: Make sure the confidentiality of electronics communication devices and restrict the interdicting and observing of communications.

(E) Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations, 2000

These telecommunication regulations provide a legal framework of lawful intrusion of communications by businesses for some specific purposes, like guarantees regulatory compliance, combating crimes or conduct investigation of illegal use of telecommunications systems. This regulation covers those conditions under which businesses can stop communications and the procedural methods to safeguard individuals' privacy.

a. Sector-Specific Regulations

Besides to the general legal framework, the UK has a sector-specific methods that assess additional privacy requirements. For example:

Financial Services: The Financial Conduct Authority (FCA) give directions to financial organizations to enables rigorous data protection measures.

Healthcare: The National Health Service (NHS) has mandatory guidelines for safeguarding patient data, ensuring the security and confidentiality.

b. Challenges and Criticisms

In spite of having a rigorous legal framework, the UK faces many challenges in the context of privacy protection:

Surveillance Concerns: Under the Investigatory Powers Act, 2016[44], the important powers given, have raised problems regarding mass surveillance and maximum abuse of powers.

Enforcement: It is also an important challenge, to enforce the execution of data protection laws across different sectors.

Brexit Implications: The UK's withdrawal from the EU has raised many uncertainties regarding the transfer of data and alignment through evolvement of data protection standards.

VI. JUDICIAL INTERPRETATION IN THE UNITED KINGDOM

In United Kingdom, the judiciary has played an important role for interpretation and execution of privacy rights. Judicial interpretation not only elaborated the importance of these rights, but

[44] Supra note 2 at 17.

have also defines the balance between user's privacy and other interests like, freedom of expression, national security and public interests. This area of this research paper defines key judicial landmarks decisions that majorly changes the privacy laws in UK, while targeting their challenges from a cyber law perspective

Malone v. Metropolitan Police Commissioner[45]

In this case of Malone vs. Metropolitan Police Commissioner establishes a major landmark in the development of privacy laws in UK. The case was filed by the Malone, whose phone was tapped by the police authority without his knowledge and consent. The European Court of Human Rights (ECHR) declares that the, there is an absence of legal safeguards against the illegally interference by the state that violates the Article 8 of the ECHR, which assures the right to respect for private and family life, home and correspondence. This case gives the guidance for essential legal frameworks that governs the surveillance activities.

Campbell v. MGN Ltd[46]

The House of Lords held in the case of Campbell vs. MGN Ltd. that deals with illegal publication of personal information regarding the Naomi Campbell's drug addiction treatment. Court held that, private individuals have a rational assumption relating to privacy regarding certain personal information, and the publication of the information shall be validated by a public interest. Under this decision, it establishes the "misuse of private information" like a tort under UK law, which balances the rights regarding privacy against the freedom of press.

Von Hannover v. Germany[47]

This case is not related with UK, but have a significant impact over the UK privacy laws. Under the case, the ECHR held that, there is a right towards public figures to enjoy her private life free from the invasion of media, unless there is a legal public interest. This case effects the subsequent UK decisions by strengthening the need to safeguard the individual's private life from the invasive media practices, also for those who are in the public eyes.

R (Wood) v. Commissioner of Police for the Metropolis[48]

The court of Appeal, under the case of R (Wood) vs. Commissioner of Police for the Metropolis, elaborates the issue of police surveillance and data retention. This case involved the police officials capturing and retaining the photographs of a peaceful protestor. The court

[45] [1979] Ch 344.
[46] [2004] UKHL 22.
[47] (2004) 40 EHRR 1.
[48] [2009] EWCA Civ 414.

held that such actions of a police officials, breaches the protestor's right to privacy under article 8 of the ECHR, highlighting that any type of interference with the privacy shall be legal and justified. This case focuses on the requirement of perceptive scrutiny of state surveillance practices.

Google Inc. v. Vidal-Hall[49]

This case of Google Inc. Vs. Vidal-Hall is concerned with the misuse of sensitive personal data through the private organization. The Court of Appeal under this case, examines the right to compensation for problems caused by a breach of data protection principles, even without any type of pecuniary loss. This judgement builds up the privacy rights in relation with safeguarding of data and sets a precedent in this digital age, relating to importance of protecting personal data.

PJS v. News Group Newspapers Ltd[50]

In the case of PJS vs News Group Newspaper Ltd., the Supreme Court reiterated the value of privacy in comparison with freedom of press, in the cases which involves the publication of personal information. In this case an injunction was passed, to stop the publication details about the extramarital affairs of the claimant. The court held that, privacy right of the claimant exceeds the interest of the public, for knowing the details of the claimant's personal life, especially it gives a major harm towards his family.

Big Brother Watch and Others v. United Kingdom[51]

In this recent case of Big Brother Watch and others vs. United Kingdom, the ECHR recognized that, the UK's mass surveillance regime violated article 8 of the ECHR because of the absence of essentials safeguards and oversight mechanisms. This decision makes a balance between national security interests with individual privacy rights.

(A) Comparative Analysis

In India and UK, the judicial interpretations of privacy rights have both similarities and differences. In India, the judiciary has increasingly expanded the scope of privacy rights with the help of landmark decisions, which gives recognition to privacy as a fundamental right. In UK, it was affected by the ECHR, which developed a rigorous legal framework related to protection of privacy through the combination of domestic and European judicial interpretations.

[49] [2015] EWCA Civ 311.
[50] [2016] UKSC 26.
[51] App Nos 58170/13, 62322/14, 24960/15 (2021).

Both of the jurisdictions focused on the need for proportionality and necessity while any invasion into the privacy, through the state or private entities. Although, the structure of the UK is being elaborated by a more structured and comprehensive legal framework, especially with the help of GDPR and the Human Rights Act, 1998.

(B) Legal Frameworks:

India

1. Constitutional Basis:

Under article 21 of the Constitution of India, the right to privacy is declared as a fundamental right, which also recognizes the right to life and personal liberty, came through the landmark decision of Justice K.S. Puttaswamy vs. Union of India. This landmark judgement was very essential in formally acknowledging privacy as included in the right to life and personal liberty.

2. Statutory Regulations:

In this digital era, the Information Technology Act, 2000 and its amendments gives a statutory legal framework for safeguarding the data and privacy. This Act includes the provisions of illegally access to computer resources, protection of data and provide penalties for data breaches.

The Digital Personal Data Protection Act, 2023, focuses on to establishes exhaustive data protection regulations, that reflected the principles that found in the Eu's GDPR.

United Kingdom

1. Constitutional and Conventional Basis:

In UK, they do not have a written constitution, although the right to privacy is being safeguard under the Human Rights Act, 1998, which comprises the European Convention on Human Rights (ECHR) into domestic law. Article 8 of the said Act, provides the right to respect for personal and family life, home and correspondence.

2. Statutory Regulations:

The Data Protection Act, 2018 includes the EU's General Data Protection Regulation (GDPR), into UK law maintain a rigorous framework against the safeguarding of data and privacy. The Act includes, principles of data processing, rights of data subjects and duty of data controllers and processors.

To regulate surveillance and interception of communications, establishes the balance between the privacy rights with national security interests, the Investigatory Powers Act, 2016 was came

into force.

(C) Judicial Interpretation:

India

1. Early Developments:

Under the right to privacy, early cases like Kharak Singh vs State of Uttar Pradesh, 1963, indicates at privacy rights but did not expressly elaborate the right. The concept of privacy came through the subsequent judgements, like Gobind vs. State of Madhya Pradesh, 1975 and R. Rajagopal vs State of Tamil Nadu, 1994, under these cases privacy becomes the right that is implicit under Article 21 of the Constitution.

2. Landmark Judgment:

The main landmark judgement under the right to privacy is the case of Justice K.S. Puttaswamy vs. Union of India, 2017, where a nine-judge constitutional bench of the Supreme Court declared right to privacy as a fundamental right. This landmark decision laid down the foundation for future related privacy legal frameworks, highlights personal autonomy, bodily integrity and informational privacy.

3. Recent Developments:

The case of Justice K.S. Puttaswamy vs. Union of India, 2018 also known as the Aadhar judgement, further reiterated the concept of right to privacy through upholding the constitutional validity of the Aadhar scheme, also imposing safeguards to safeguard individual's privacy.

United Kingdom

1. Influence of ECHR:

In the UK, the judicial interpretation of the right to privacy has been affected by the ECHR and the Human Rights Act, 1998. Other cases like Malone vs. Metropolitan Police Commissioner, 1979 and Campbell vs. MGN Ltd. 2004 has reiterated the safeguarding of privacy under Article 8 of the ECHR.

2. Balancing Act:

The courts of UK have continuously elaborated the balance between the privacy rights with other interests like freedom of expression and public interests. The decision held in the landmark case of Campbell vs. MGN Ltd. establishes the tort of misuse of private information, balancing the privacy of individual against the freedom of press.

3. Surveillance and Data Protection:

Landmark cases as R (Wood) vs. Commissioner of Police for the Metropolis, 2009 and Google Inc. vs Vidal-Hall, 2015 have discussed the complications of privacy in relation with state surveillance and data protection.

4. Recent Developments:

In the case of Big Brother Watch and Ors. Vs. United Kingdom, 2021, the ECHR gives decision that censure the UK's mass surveillance regime, also focuses on the requirement for adequate protection and other mechanism to safeguard individual's privacy.

(D) Comparative Insights:

1. Recognition and Scope:

Right to privacy is recognized under both the countries i.e. India and UK, but in India Article 21 of the constitution recognize privacy as a fundamental right, which gives a broader concept of privacy as compared with the UK's framework.

2. Data Protection:

The GDPR is adopted by the UK through the Data Protection Act, 2018 sets an high standard for the protection of data, with having exhaustive rights for data subjects and rigorous conditions for data controllers. Personal Data Protection Bill which is still pending focuses on the same standards.

3. Surveillance and State Interference:

Both the countries have the rigorous legal framework that regulates state surveillance, but the Investigatory Powers Act, 2016 has faced difficulties for giving exhaustive powers towards intelligence agencies. In India, legal frameworks have to balance between national security with individuals' privacy, as we seen in the Aadhar judgement.

4. Judicial Approach:

The judicial approach in both countries emphasizes proportionality and necessity in any interference with privacy rights. However, the UK's reliance on the ECHR provides an additional layer of protection through the oversight of the ECtHR.

(E) Challenges and Future Directions

Many problems and difficulties have been encountered in the case of the right to privacy, especially in the context of the digital world where the latter is still in development to overcome the problems faced by it. However, the factors such as geopolitical factors, social-cultural

factors, and advancements in technology along with important Court judgments are some of the other factors which make up a complex environment in India & UK. Discussing the subject from the perspective of cyber law, this section identifies the main challenges and probable future shifts in the privacy law in the two countries.

a. Technological Advancements

1. Big Data and AI:

Privacy threats are evident when big data and AI are applied on a large scale. Many people fall victims of advanced analytics and machine learning to infer their Sensitive personal information often without their permission. New technology needs to be regulated in the UK and India and this can only be achieved through legal jurisdictions, thus preserving privacy.

For instance, concerns over prejudice and misuse are voiced over the uses of AI in surveillance and predictive police. Therefore, effective measures are provided in these challenges by the functional and comprehensive legislation.

2. Internet of Things (IoT):

Data security and especially privacy are hence experienced as being harder to achieve due to the growth of the Internet of Things, as well as the vast amounts of data that are collected from these devices. New legislations have to be created to dictate how linked devices pose unique risks.

The problem of assuring the high level of security and clarifying responsibilities in case of the leakage of the personal information is especially acute in the context of the IoT ecosystems.

b. Regulatory and Enforcement Issues

1. Fragmented Regulations:

- Where India does not have a data protection law similar to the GDPR in the UK, it means that the regulatory frameworks are fragmented. While the Digital Personal Data Protection Act of 2023 is encouraging, it became an Act of parliament and enforced in the right spirit.
- In other words, while the UK no longer falls under the jurisdiction of GDPR, which is a part of the EU, then there are issues regarding data protection especially touching on cross border transfers.

2. Enforcement Mechanisms:

- Both countries appear to have serious issues in the implementation of their privacy

regulations. For this, the organisations like Information Commissioner's Office, United Kingdom or the emerging Data Protection Authority, India needs to be empowered with adequate authority and funding.

- Further, the conservative public will not commit to digital selves and technologies unless authorities respond swiftly and effectively to threats and violations of the tenet.

c. Surveillance and State Powers

1. Mass Surveillance:

- The very act of Investigatory Powers in the United Kingdom approved in 2016 has been criticised for allowing broad surveillance, following the problems with the control of powers and their proportionality. A major challenge that has remained however is determining whether the specific methods of surveillance are compliant with human rights.
- The apprehensions about state agencies' monitoring in India without adequate supervisory checks point to the need for transparent and Check This Out? procedures.

2. Balancing Security and Privacy:

- The idea of achieving privacy in one's life and security for the nation frequently produces issues. Both nations must navigate these challenges very prudently so as not to compromise the right to the privacy of the people than is necessary.

d. Global and Geopolitical Factors

1. Cross-Border Data Transfers:

- Since data flow is international in nature, because in brief, harmonised legislation is needed to allow cross border data transfer while offering data protection. Different regulatory standards, as it is seen, might harm people and businesses, make them somehow insecure, and put them in a disadvantageous position.
- They have to make certain that it respects the international requests, for instance, GDPR, and address the issues of data transfer after Brexit. Similarly, to adapt its laws to the international standards for enabling cross border data flows, India needs to give the necessary harmonisation.

2. Cybersecurity Threats:

- The general public faces severe privacy risks due to increasing tendencies of Cybersecurity threats, including data and cyber-attacks. That is why the population of

both nations needs the adherence to high levels of cybersecurity to protect against the misuse of and unauthorized access to, personal information.

- That is why, the legislation of an effective privacy protection policy should also include the introduction of severe penalties for cybercriminals and increasing awareness of cybersecurity among the population.

(F) Future Directions:

a. Legal and Regulatory Reforms

1. Comprehensive Data Protection Laws:

- Finally, to capture a holistic approach towards data protection, it is high time for India to pass and implement the Personal Data Protection Bill, 2019. This includes specific provisions for data processing, data subject's rights, and measures in relation to data controllers and processors.
- Although Brexit has introduced regulatory changes to the UK, the country needs to maintain the relevant legislation to address new developments and ensure compliance with the international norms.

2. Regulation of Emerging Technologies:

- Prototype legislation on big data, IoT, and AI and other progressive technologies must be formulated by both states. These rules should deal with issues of accountability, equality, and openness in respect of data.
- Some of the first tasks are to set an ethical framework for using AI, and guarantee that Iot devices are regulated with the best security laws.

b. Strengthening Enforcement Mechanisms

1. Empowering Regulatory Bodies:

- Thus, improved capacities of the existing and emerging data protection authorities including the ICO in the UK and the proposed Data Protection Authority in India are crucial. This requires adequate financial support, technical expertise, and enforcement power that ensures compliance with data protection laws.
- Enhancing interaction between the global and domestic legal entities might increase the effectiveness of the measures applied.

2. Promoting Public Awareness:

- There is a need to increase awareness of the public on protection of their data and their

privacy rights. The people should be provided with the resources and the awareness on how to exercise their rights and protect their information.

- Organizations can ensure that they have more privacy consciousness by raising consciousness levels through encouraging companies to adhere to privacy by design and through the regular conducting of privacy impact assessments.

c. **Enhancing Oversight and Accountability**

1. Transparency in Surveillance Practices:

- Both nations require the certain that the amnesty methods of surveillance are public and regulated stringently. It is suggested that independent organisations should investigate the monitoring activities and ensure people's right to privacy not to be violated intentionally.
- Accountability can be increased by means of judicial control and requiring reporting on the measures taken in the sphere of surveillance.

2. International Cooperation:

- There is therefore need to advance international cooperation on issues of privacy and data protection. To synchronise laws and liberalise cross border data transfer both the countries should bilaterally negotiate and sign with other countries.
- Concerted efforts can be made on the domestic level to advance protection of privacy rights through participating in the international conventions and gaining knowledge from different countries' practices.

d. **Addressing Cybersecurity Challenges**

1. Robust Cybersecurity Frameworks:

- There is a dire need to develop and implement strong cybersecurity measures that will ensure the mitigation of threats which compromises people's data. In this, implementation of the latest security technologies, periodic scan for weaknesses and presence of incident handling procedures are employed.
- Coordination between the public and the commercial side can raise defensive levels on average.

2. Stringent Penalties for Cybercrimes:

- Affine sanctions that are imposed for cybercrimes and data breaches can motivate compliance with data protection regulations and discourage malicious actions. Since

the public needs to have their trust in the legal systems, it is equally important to guarantee an efficient and speedy legal process against offenders.

- The authorities should arm the law enforcement organisations with the requisite tools, training and teach them on how they can effectively fight cybercrimes.

VII. CONCLUSION

Hence, to sum it up, the legal position of privacy in India is a fluid one that is constantly evolving. Despite the progress that has been observed mainly in the form of judicial initiatives and legislative bills, further enhancement of the requirements for the enforcement of the legislation and the strengthening of the corresponding bodies are needed. Hence, it was clear that the protection of privacy rights in India would require frequent changes and awareness as technology evolves.

The legal framework of privacy in the United Kingdom is characterized by its complex and heavily legislatively controlled system, reinforced with a persistent regulatory control and focus on the subject's rights. Although the position of the United Kingdom concerning protection of individuals' privacy has significantly improved over the recent years, new challenges in the age of big data and cloud-based services will always arise and thus need proper attention and consideration.

Studying each of these works provides a holistic understanding of practically all the facets of privacy law in India and the UK. First, they give historical information, secondly, they offer some tips, and thirdly they give perception on how some laws on privacy impact the society. In turn, the research could use the present bodies and viewpoints and enrich the analysis of the right to privacy in both jurisdictions placing the findings into the frame of the present literature.

Analysing the differences in privacy laws of India and the UK sheds light on how courts of the two regions engage with each other in the process of law. However, both countries have achieved significant improvements in the protection of privacy; nevertheless, there are some challenges that they face regarding the rapidly growing world of technologies. Policies related to the privacy of information will be defined by the changes of legislation and legal precedents in both regions regarding cyber law in the future.

The right to privacy in India and the UK faces several challenges, which make it necessary to adapt the legal system and judges and lawyers' approaches. In essence, both nations need to tackle global factors, legal issues, enforcement perspectives, and technological enhancements if they have to adequately defend private rights. The prospects to be followed are legal

transformations both extensive and intensive, enhanced supervision and monitoring, strengthening of measures for law enforcement and implementation, and the use of IT safety techniques. India and the UK might ensure that privacy rights are honoured in a world that is turning into the digital one by overcoming such barriers and looking to the future.

*****

 [ISSN 2581-9453]

VIII. REFERENCES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. Human Rights Act, 1998.
3. Data Protection Act, 2018.
4. Cofone, Ignacio. The privacy fallacy: harm and power in the information economy. CambridgeUniversityPress,2023.https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=the+privacy+fallacy+by+Ignacio+&btnG=#d=gs_cit&t=1722362989095&u=%2Fscholar%3Fq%3Dinfo%3AeqMvNRwDJrwJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den
5. Wright, D., & De Hert, P. (Eds.). Privacy and Data Protection: Challenges of Modern Information Technologies. Springer. 2012.
6. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
7. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
8. Information Technology Act, 2000, Section 43A.
9. Information Technology Act, 2000, Section 72A.
10. Indian Penal Code, 1860, Section 354C.
11. Digital Personal Data Protection Act, 2023.
12. K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.
13. Reserve Bank of India guidelines; Insurance Regulatory and Development Authority of India guidelines.
14. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
15. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
16. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
17. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
18. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
19. Malone v. Metropolitan Police Commissioner, [1979] Ch 344.
20. Campbell v. MGN Ltd, [2004] UKHL 22.
21. Von Hannover v. Germany, (2004) 40 EHRR 1.
22. R (Wood) v. Commissioner of Police for the Metropolis, [2009] EWCA Civ 414.

 [ISSN 2581-9453]

23. Google Inc. v. Vidal-Hall, [2015] EWCA Civ 311.

24. Big Brother Watch and Others v. United Kingdom, App Nos 58170/13, 62322/14, 24960/15 (2021).

25. Data Protection Act, 2018.

26. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

27. European Convention on Human Rights, Article 8.

28. Investigatory Powers Act, 2016.

29. Privacy and Electronic Communications Regulations (PECR), 2003.

30. Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations, 2000.

31. Financial Conduct Authority guidelines on data protection.

32. National Health Service data protection guidelines.

33. Malone v. Metropolitan Police Commissioner, [1979] Ch 344.

34. Campbell v. MGN Ltd, [2004] UKHL 22.

35. Von Hannover v. Germany, (2004) 40 EHRR 1.

36. R (Wood) v. Commissioner of Police for the Metropolis, [2009] EWCA Civ 414.

37. Google Inc. v. Vidal-Hall, [2015] EWCA Civ 311.

38. PJS v. News Group Newspapers Ltd, [2016] UKSC 26.

39. Big Brother Watch and Others v. United Kingdom, App Nos 58170/13, 62322/14, 24960/15 (2021).

*****

 [ISSN 2581-9453]