|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

|LAW AUDIENCE JOURNAL®|

|VOLUME 2 & ISSUE 1|

|ISSN (O): 2581-6705|

EDITED BY:

LAW AUDIENCE JOURNAL'S

EDITORIAL BOARD

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

Email: lawjournal@lawaudience.com, info@lawaudience.com,

Phone: +91-8351033361,

Website: www.lawaudience.com.

Facebook: www.facebook.com/lawaudience

Instagram: www.instagram.com/lawaudienceofficial

Contact Timings: 5:00 PM to 9:00 PM.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

DISCLAIMER:

This article is published free of cost as a part of ***Law Audience's 4th National Online Essay Writing Competition 2020.*** *No separate Article Processing Fee is charged. Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in* ***Volume 2 & Issue 1*** *are the original work of the authors.*

Views or Opinions or Suggestions ***(if any)****, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.*

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

"DIGITAL PRIVACY: SIGNIFICANCE AND ITS SURVEILLANCE."

AUTHORED BY: MR. MD ZEESHANUZ ZAMAN (B.A.LL.B),
UNIVERSITY OF CALCUTTA, DEPARTMENT OF LAW,
EMAIL ID: MDZEESHAN2810@GMAIL.COM.

I. ABSTRACT:

"This paper explicates the Constitutional provision encompassing the Right to Privacy and its apprehensive breach through inordinate surveillance. The Right to Privacy can be vividly discerned as enshrined under Article 21 of the Constitution of India. The paper elucidates on the precariousness of privacy in the digital world and the advent of administrative surveillance on technological platforms. It briefly exposes the significance of perpetuating equilibrium between the facets of digital privacy and its inevitable surveillance. The author attempts to highlight the urgency of bringing in appropriate oversight mechanisms in order to secure personal data."

II. INTRODUCTION:

The right to privacy derives its interpretation from an English Common Law maxim which states that "***Every man's house is his castle."***[1] Before delving into the intricacies of the aforesaid right, it is pertinent to have a basic conception of what privacy is all about. Privacy is that invisible demarcation that segregates our actions and emotions from undesired interventions. Every individual has a distinctive set of thoughts, interests, perceptions which remain confined within an exclusive zone and is not meant to be publicised. Privacy is undoubtedly an integral part of any human interaction or relation, and any sort of meddling into such affairs has its repercussions. U.S. Supreme Court Justice Louis D. Brandeis had expounded the law of privacy and in a celebrated judgment had said that right to privacy is

[1] R. v. Stevens, 2011 ONCJ 794, 35.

"the right to be let alone…the right most valued by civilized men."[2] The Black's Law Dictionary similarly defines the right and further asserts the right to privacy as a right to live without unwarranted interference by the public in those matters which do not necessarily concern them[3]. It is an aspect that has enkindled innumerable deliberations and its interpretations in legal parlance have stirred up major implications in society. It is most definitely an integral part of an individual's life and its ubiquitous influence is quite perceptible.

III. INDIAN SUPREME COURT: RIGHT TO PRIVACY IS A FUNDAMENTAL RIGHT:

A close perusal of the supreme law of the land evinces the fact that the Indian Constitution does not explicitly allude to the right to privacy. Nevertheless, it can be vividly ascertained that the wide ambit of the right to freedom of speech and expression does include the aspect of the right to privacy. Personal liberty enshrined under Article 21 of the Indian Constitution covers a vast domain of rights which unequivocally encompasses human dignity, secrecy, autonomy and many other facets. Every person is legally entitled to personal liberty which can only be curtailed by a procedure established by law.

In most nations, the Constitutional modes of safeguarding individual privacy have either been enumerated in some legal enactment or it has been propounded in the Court of Law. The enforcement of such rights has strongly hinged upon the factual scenario and the encapsulating moral principles. In the landmark case of ***R. Rajagopal v. State of Tamil Nadu***[4]**,** the Supreme Court of India had held that the right to privacy is a right to be let alone. It interdicts the publication of any matter without the consent of the individual with whom it is concerned. The absence of an explicit elucidation of the right to privacy in the Indian Constitution has often led to incongruent legal propositions. Eventually, on 24th August 2017,

[2] Joel K. Goldstein & Charles A. Miller, *Brandeis: The Legacy of a Justice*,100 Marquette Law Rev. 462, 473 (2016).
[3] BLACK'S LAW DICTIONARY 1315 (9th ed., 2009).
[4] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

in the landmark judgment of ***Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.***[5], the Apex Court had held that the right to privacy is protected as an inherent part of the right to life and personal liberty under Article 21 of the Constitution of India and as a part of the freedoms guaranteed by Part III of the Constitution. It was held that, **"*Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III.*"**[6]

The path-breaking judgment has overruled the decisions pronounced in preceding cases such as ***M. P. Sharma & Ors. v. Satish Chandra & Ors.***[7] **and** ***Kharak Singh v. State of U.P. & Ors.***[8]. The safeguard of this right will play a very crucial role in inhibiting the misuse of the Right to Information Act, which has been persistently utilized as a weapon to infringe the privacy of individuals in the name of transparency.

IV. THE ADVENT OF DIGITAL PRIVACY:

Modernisation has effectuated an intricate transformation in the aspect of global connectivity and has quite covertly dispersed its roots into the lives of people. The newly incorporated technologies have paved the way for third parties to access the basic information of citizens and manipulate them accordingly. It is not only the physical matter but also the intellect and emotions of people that stand exposed without any kind of self-realisation. The era of digitalisation has empowered every sector to store and disseminate data which in turn has accelerated their covert assimilation with the personal profiles of citizens.

Since the colonial epoch, every incumbent government has codified and effectuated various statutes to bring about momentous reformations in the realm of surveillance. During the era

[5] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
[6] *Ibid* at 320.
[7] M.P. Sharma & Ors. v. Satish Chandra & Ors., AIR 1954 SC 300.
[8] Kharak Singh v. State of U.P. & Ors., (1964) 1 SCR 332.

of colonial subjugation, the Indian Telegraph Act, 1885[9] and the Indian Post Office Act, 1898[10] were enacted for such purpose. These legislations were considered to be the cradle of surveillance in the country. Subsequently, the Information Technology Act, 2000[11], came into force which sanctioned government surveillance on digital platforms. In the year 2009, new rules and regulations were formulated to keep an eye upon the data and metadata.

In the case of ***Gobind v. State of M.P. & Anr.***[12], Justice Mathew had asserted that the right to privacy was itself a fundamental right, but at the same time was subject to certain restrictions on grounds of public interest. Nonetheless, in December 2018, the central government came under the radar of intense condemnation, after ten governmental agencies including the Delhi Police Commissioner were endowed with unprecedented surveillance powers[13].

Such a debatable move was undertaken just a few months after the Apex Court had declared the right to privacy as a fundamental right. Although individual privacy is regarded as a rudimentary right to which every citizen is legitimately entitled, there are instances when it might be imperative for the government to transcend such legal entitlement of the commoners.

Certain unforeseen circumstances might pose an imminent threat upon the national security, and in such situations, the concerned authorities might be devoid of any worthwhile alternative. However, it is well perceived that both use and abuse go hand in hand. It is highly infelicitous, albeit a harsh reality that most often the incumbent leaders holding ministerial positions and bureaucrats exploit such authorised sanctions to curb any form of dissent against the ruling authority.

[9] The Indian Telegraph Act, 1885, Act No. 13 of 1885.
[10] The Indian Post Office Act, 1898, Act No. 06 of 1898.
[11] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000.
[12] Gobind v. State of M.P. & Anr., (1975) 2 SCC 148.
[13] NH Web Desk, *India becomes a surveillance state; Modi govt authorises agencies to snoop on citizens*, NATIONAL HERALD, (Dec. 21, 2018, 02:09 PM), https://www.nationalheraldindia.com/india/india-becomes-a-surveillance-state-modi-govt-authorises-agencies-to-snoop-on-citizens.

V. EXIGENCY OF SAFEGUARDING DIGITAL PRIVACY IN THE COURSE OF SURVEILLANCE:

Delving into the aspect of informational privacy, Alan Westin in his classic book ***"Privacy and Freedom"*** has given the most thoughtful exposition of the interests that have been at stake in the matter of data protection[14]. Westin has portrayed the concern for privacy as something intricately subjective, where people themselves determine as to what extent they would desire their attitudes and their ideas to stand exposed.

There exists a fine line of demarcation between the protection of individual privacy and the extent of state intervention in such matters. In an interview, Justice B.N. Srikrishna, the person who had been at the forefront of the drafting committee of The Personal Data Protection Bill, 2018, had emphasised on the need to draft a law that would regulate how the government and its agencies monitor the citizens by employing technological means[15]. Under the present legal framework, all it takes to conduct surveillance is a mere nod of the Secretary, which manifests the necessity of introducing proper mechanisms for judicial scrutiny.

Privacy is an essential component of human dignity and every individual is entitled to express their opinions and thoughts to the person they wish to, without any sort of intervention by the state or private corporations. However, such a right has often been viewed as an impediment by the government, which has always tried to legalise its infiltration into private data by the enactment of laws under the garb of ensuring public tranquillity. When an individual shares certain personal information concerning their actions or emotions with another person, it is done with the intent to convey it personally. Now, if such data is exposed to the views of the state without the consent and knowledge of such a person, then it should not be called surveillance but a deliberate leak.

[14] Merri Beth Lavagnino, *Informational Privacy Revealed*, 48 EDUCAUSE Rev. 11, 12 (2013).
[15] Megha Mandavia, *Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna*, THE ECONOMIC TIMES (Dec. 12, 2019, 11:34 AM), https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr.

We need to realise that a magnanimous amount of information is available across the internet. In the present digital era, information that is collected by the different applications and the associated companies have significant commercial value and such data unknowingly enters into a vicious loop whereby they are continuously circulated among multiple organisations. Most of the private corporations keep a track on the data which is shared and searched by the citizens, which in turn, are easily available at the disposal of the state authorities. The lack of adequate regulations with respect to the handling of such data has made personal human connectivity vulnerable. The accessibility of such private conversations reveals how conspicuously the freedom of speech and expression is being compromised.

The alarming level at which the government has been spying upon the personal lives of citizens has made people realise the necessity to censor even a private interaction. It has more often been seen that the large corporations sell the data to other companies within the global network for their own commercial purposes. Based upon the searching habits of a user, other websites often adjust their associated advertisements.

This also promotes a discreet form of societal discrimination as the companies get to manipulate and indirectly influence the type of advertisements one is exposed to. Quite covertly but effectively, they creep into the psyche of the common people and mould their basic understanding of products and services.

Jennifer Stisa Granick, an American Attorney has said, ***"This idea that you can be manipulated into seeing, believing, buying and thinking things that aren't what you normally would do — and nobody knows about it because nobody knows what I see is different from what you see — is scary."***[16] She has time and again voiced her opinion on the consequential issue for which Senator Ron Wyden has called her an "NBA all-star of surveillance law."[17]

[16] Yasmin Belkhyr, *The terrifying now of big data and surveillance: A conversation with Jennifer Granick,* TED Blog (Oct. 1, 2019, 05:44 PM), https://blog.ted.com/the-terrifying-now-of-big-data-and-surveillance-a-conversation-with-jennifer-granick/.
[17] *Ibid.*

It is further imperative to explore the wide ambit of implications that has been brought about by such unwarranted infringements. Certain professions demand privacy as their fundamental requisite and its hindered availability acts as a serious obstruction in their effective functioning. Journalists and activists are often in pursuit of critical information as they work on high profile cases involving influential personalities. The political leaders often exert their influence so as to espionage into facts that might expose their mishandlings and financial embezzlements. Under such circumstances, any breach or leak in such journalistic investigations can pose serious threats upon the lives of these people. The broader spectrum of privacy also includes the right to free speech which can only be protected and promoted if the citizens have the secured means to interact without the fear of being unnecessarily watched. In a society where democratic ideals are so meticulously talked about and revered, the presence of a fearless platform of criticism is indispensable.

Such apprehensions call for immediate judicial intervention and it also emphasises on the need for transparent documentation of every digital surveillance to ensure that they are only availed if such necessary circumstances arise. Several petitions have been filed before the Apex Court, questioning the constitutionality of the existing surveillance laws. The intervention of the judiciary and its subsequent impact upon the existing laws has always been the epicentre of solace for the victims of abuse.

In the United States, electronic surveillance is considered to be a search under the Fourth Amendment which protects individuals from unreasonable search and seizure. Therefore, it is indispensable for their government to obtain a warrant from the court before conducting a search to establish the legitimacy and absolute necessity of such a search. Notwithstanding the incumbent rules and regulations, in India, rampant violations of such codifications continue to subsist under the garb of enforcing law and order. Every ruling party has/have encountered scathing criticism for implementing unwarranted and unjustified surveillance upon the lives of ordinary citizens. Recently, the proliferation of the malware named Pegasus

created a huge furore across the nation[18]. The government was accused of cyber espionage due to the hacking of social media accounts of several activists and lawyers who were eminent for voicing their opinions of dissent and for unveiling the dereliction of duty on the part of the government.

Thereby, one can also expound upon the necessity to form an oversight board which shall not be responsible to the government but to a judicial authority. The governmental agencies, as well as the private corporations, shall be accountable to such board whenever an explanation is asked for. It will ensure absolute transparency on matters of data sharing and will prevent all sorts of unjustifiable intrusion into the privacy of citizens.

It is palpable that the state's Intel agencies cannot remain totally ignorant of the digital transmissions, but at the same time, it is crucial that proper justification is handed over if such surveillance is ever brought to question. It is perceptible that complete transparency would paralyse the functioning of Intel agencies and moreover, publicising such classified information would sorely affect the confidential operations. With persistent terror alarms, it is obligatory on the part of the Intel services to conduct regular interceptions, and such investigations demand covert protocols. Since they are answerable in cases of any intelligence failure, it is for this reason that a certain degree of data infringement on their part is justifiable and excusable. Nevertheless, there are different ways, such as, traffic analysis and content filtering by which the authorities need not peruse the entire information of an individual and a positive decision can be taken by harnessing the peripheral data. The adoption of such mechanisms is highly warranted since they serve the basic purpose of surveillance without over-indulging into the privacy of people.

Nevertheless, the law`s ambivalence regarding the issue of administrative surveillance has made it susceptible to a wide ambit of loopholes. It is really complex to figure out the necessity of the administrative operations and adjudge whether such actions have any

[18] Anindita Singh Mankotia & Megha Mandavia, *After Pegasus spying row, India asks WhatsApp to explain privacy breach***,** THE ECONOMIC TIMES (Nov. 02, 2019, 02:55 PM), https://economictimes.indiatimes.com/tech/internet/after-pegasus-spying-row-india-asks-whatsapp-to-explain-privacy-breach/articleshow/71851802.cms.

justification with respect to the associated context. The present scenario calls for judicial intervention and a critical analysis of the present guidelines concerning such an overseeing mechanism. Under such circumstances, it is imperative that the judiciary maintains its ascendancy over the two other wings of the government. The courts have many a time lambasted the unnecessary infringement of the privacy of individuals.

Every governmental agency should strictly adhere to the protocols and regulations to prevent any arbitrary application of power. Surveillance measures must never be intertwined with any form of discretionary power.

VI. CONCLUSION:

In the landmark case of ***Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.***[19], the Supreme Court of India had laid down that, ***"Privacy has both positive and negative content. The negative content restrains the State from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the State to take all necessary measures to protect the privacy of the individual."***[20] National Security is certainly the raison d'etre of administrative surveillance, but at the same, it is necessary to ensure that the latter does not engender a virtual panopticon. It is perceptible that a breach in such platforms shall infringe the private data of millions.

Simultaneously, it is pertinent to note that a constitutional right can never be the panacea for resolving privacy issues. It is the government's cardinal obligation to ensure considerable mechanisms to safeguard the right which is desperately yearned by all. In the end, we can just anticipate a credible balance between the interests of individuals and that of the society at large.

[19] (2017) 10 SCC 1.
[20] *Ibid* at 326.