Page 1107 - 1112 **DOI:** *https://doij.org/10.10000/IJLMH.113453*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 4

2022

National Security vs. Right to Privacy: A Conflict of Interests

PUSHYA CHHABRIA[1] AND HIYA GANDHI[2]

ABSTRACT

Purpose: *This study highlights the grey area between national security and the individual right to privacy.*

Research implications: *This research offers a preliminary understanding of the proportionality between the right to privacy of an individual and Government surveillance for national security purposes.*

Findings: *The primary reason behind the existence of grey areas between national security and individual right to privacy is the unclear laws that regulate our nation. WhatsApp filed a petition before the Delhi High Court, contending the intrusion of the Indian Government to trace the originator of a particular message, could severely hamper the fundamental rights of the citizens. This would not have happened if India had proper laws and legislations that governed data protection and the right to privacy.*

Originality and value: *This article also provides action-based solutions to eliminate grey areas in the field of surveillance. Aarogya Setu, Pegasus and other real situations have been analysed in this study.*

Keywords: *Right to privacy, national security, data protection laws, Aarogya Setu.*

I. INTRODUCTION

With growing technological advancements, the risk of privacy breaches and unjustified surveillance has made its way, surpassing the unclear laws and rules pertaining to data privacy. In 2017, right to privacy was guaranteed as a fundamental right to the citizens of India, but no stringent laws were made to protect such fundamental right. Back in the day, barging into someone's personal data was considered to be one of the most difficult tasks, by virtue of backwardness of the country in terms of financial and technological resources. Reduced financial constraints and technological advancements have opened ways for unjustified surveillance. There has been a constant conflict of interests between the Government and the citizens of India, owing to the unclear regulations that create a grey area. This conflict of interests arises with the need for Government surveillance to maintain national security and the

[1] Author is a student at Kirit P. Mehta School of Law (NMIMS), Mumbai, India.
[2] Author is a student at Kirit P. Mehta School of Law (NMIMS), Mumbai, India.

 [ISSN 2581-5369]

justified demand of citizens to protect their right to privacy. In several instances, the Government of India has encroached into the private data of citizens online, relying on the sole justification of 'national security'. This article aims to highlight such instances and provide feasible solutions to eliminate this grey area.

(A) Research Question:

Do National Security and Right to Privacy prevail and mutually exist at the same time?

(B) Research Objectives:

1. Evaluating the grey area between National Security and Right to Privacy.
2. Analysing the functioning of the Government app 'Aarogya Setu'.
3. Providing potential solutions to strike a balance between national security and the privacy of an individual.

II. ANALYSIS:

During Justice K. S. Puttaswamy (Retd.) and Anr vs. Union Of India And Ors in 2017, the apex court delivered a landmark verdict which guaranteed right to privacy as a fundamental right to the citizens of India, under Articles 14, 19 and 21 of the Indian Constitution. However, our legal framework is still incipient in terms of safeguarding this fundamental right. There has been a constant conflict of interest between national security and the individual right to privacy.The primary reason behind the grey area created between national security and right to privacy is the unclear laws and statutes of our country. For instance, traceability by the State isn't clearly defined under Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021. In fact the term 'national security' is not defined either, not even in the National Security Act, 1980. Although, in a 2017 hearing, The Honourable Supreme Court cautioned the Government that traceability must be only under 'special circumstances' that threaten the security and sovereignty of India. Moreover, the Government must ensure that no breach of individual right to privacy occurs while performing such actions. However, the Government was allegedly compelling the social media giant to provide the Government the ability to trace originators of messages shared on the said platform. Similarly, Pegasus- an Israeli spyware, developed to read encrypted messages and tap phone calls was used in India in the name of 'national security'. Section 66 read with Section 43 of the IT Act, 2000, forbids the hacking of a device. Furthermore, Section 69 of the IT Act, 2000 authorizes the Government to trace information for the purpose of national security but it does not permit any agency-national or private-to use spywares for the same. This creates a grey area between national security and the fundamental right to privacy. A petition was filed by WhatsApp before the Delhi High

 [ISSN 2581-5369]

Court, contending the intrusion of the Indian Government to trace the originator of a particular message. The social media giant argued that this would require de-encryption of the messages shared on its platform, and that could severely hamper the fundamental rights of the citizens. Nevertheless, India's existing surveillance laws are of utmost importance to protect the interests and integrity of the country. Section 69 of the IT Act, 2000 is one such law which empowers the Central Government and its agencies to intercept and monitor information transmitted or received on a device, for valid reasons, such as curbing criminal activities and terrorism. While surveillance acts as a deterrent for cybercriminals, it is also important for the laws in India to confer restrictive powers to the Government to ensure that the fundamental right of citizens is not breached in the process of surveillance. Enunciating proper definition of laws is of the need of the hour to eliminate the grey area and negotiate a balance between national surveillance and the individual right to privacy.

III. CASE STUDY

Once again, the Government was torn down in striking a balance between national security and a citizen's privacy. The pandemic hit in 2019 and became a health emergency. In April 2021, the Government came up with the app "Aarogya Setu", which the Government used to spread awareness about COVID as well as link people with health services. What the Government also did with this app is keep a track of people infected by COVID, they wanted to see if a geographical area was being clustered by many cases and this used the Bluetooth and location service of a person's phone. Soon questions were raised as to too much data was being collected by the Government through this app and the Government was keeping track of its people through this which basically encroached a person's privacy. There were several issues that were raised by the public that this app breaches their right to privacy. An open-source app is when the code of the app is available to the people to review and scrutinize it, it was highly criticized that despite a Government policy that all the apps by the Government of India should be open sourced Aarogya Seta was not. The terms and conditions of the app had also mentioned that the Government would have no liability if the data of a person was leaked through the app. People even started doubting the purpose of this app, what if the Government was selling their information or using it for unethical purposes. The sites which collect data are only allowed to retain it for 180 days, but the Government said that if they collected any reports or datasets, they could withhold it for purposes needed to help them assist public in the pandemic, but who knows if they retain it or use it even after the pandemic and who will keep a check on this? The app is also very prone to data breaches, a French ethical hacker Elliot Alderson said that he could access files of the app, he could see where which person was infected and users' locations

 [ISSN 2581-5369]

were exposed. Therefore, making it clear that the app was not safe and secure. This again boils down to a mere proportionality test between where national security and health of the nation was concerned vs. the privacy of its citizens. This shows the dire need of India to work on its data security and privacy of its citizen so that all Indians are given their right to privacy as guaranteed by Article 21 which ensures life with human dignity and personal liberty of the Constitution and as rightly said by Justice D Y Chandarachud that there is no dignity without privacy.

IV. RESEARCH SUGGESTIONS

1. The most important reform being that in this age of digitalisation where every other country has strict laws on privacy and data protection, India does not even have a proper legislation in place. The government should work on making proper and strict legislations, laws and rules to protect its citizens' privacy and to make the digital space safe.
2. The United Nations has so many bodies and in this world where everything is shifting online, it should form a separate body for data protection and right to privacy and keep a check on each of its member nations and its government if they are protecting and taking actions towards this.
3. There should be a separate committee set up which comprise of IT specialists, ethical hackers and advocates to approve that the site or government app is safe before it is launched for the public.
4. If the government launches an app it should make clear the purpose and use of the app to the public as it is a democracy and there are no suspicions in the mind of the people. It should also make an announcement as to what documents will be required by the site or app so that people don't get robbed of their privacy by fake websites or due to the mere reason that they were uninformed.

V. CONCLUSION

Are you actually given the fundamental right you are promised? Apparently, No. The Government who has given these rights to you at times encroaches upon it. One of the main reasons being that the same Government has given this right but has not worked on its execution as to how they will protect this right to privacy in a digital space. There are no rules leave aside laws and legislations. Government can just launch a site or an app without proper information as to what the site does or what information it is authorised to collect and why. Government can keep taking information of its citizen with the reason that it's for national security and at the

 [ISSN 2581-5369]

same time breach ones privacy. This is going to remain a grey area until laws and stricter regulations are formed and enforced by the Government.

*****

 [ISSN 2581-5369]

VI. REFERENCES

Statutes:

1. Information Technology Act, 2000, Acts of Parliament, 2000 (India)

Online Sources:

2. Aditya Verma, *Right to Privacy*, Central Information Commission (cic) 2, 4-20, (2019), https://cic.gov.in/sites/default/files/Right%20to%20Privacy%20and%20RTI%20by%20Aditya%20Verma%20%20%281%29%20%281%29.pdf
3. Tathagata Satpathy, Karnika Seth, Anita Gurumurthy, *Are India's laws on surveillance a threat to privacy?*, THE HINDU (Jan. 3, 2022, 5:30 PM), https://www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25844250.ece
4. The Times of India, *Is Aarogya Setu stealing your data? Several experts think so: CNN*, THE TIMES OF INDIA (Jan 5, 2022, 3:50 PM), https://timesofindia.indiatimes.com/blogs/foreign-media/is-aarogya-setu-stealing-your-data-several-experts-think-so-cnn/.

*****