INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 2 | Issue 4 [2024] | Page 100 - 102

DATA PRIVACY VS SECURITY: A QUEST TO HARMONIZE THE TWO PRIORITIES

- **Karan Dhoria**[1]

In the age of digitalization, data protection is a growing concern as data privacy and security issues have grabbed public attention across the globe. There have been innumerable instances where an individual's right to privacy has conflicted with issues concerning national security. The long-standing debate of privacy vs national security became more pronounced in India after the introduction of the Adhaar Act. Adhaar – a biometric identity system that provides every Indian citizen with a unique identification number to enable certain government services. Privacy activists have argued that consolidating biometric data violates an individual's right to privacy as it increases the likelihood of identity theft and surveillance. On the other hand, the government has guaranteed that the information collected is safe and used only for specific purposes to provide certain services to the public. Based on these contentions, a nine-judge bench of the Supreme Court held in Justice K.S. Puttaswamy (Retd.) vs The Union of India that the right to privacy is indeed a part of Article 21 of the constitution. Justice D.Y. Chandrachud went ahead to say that dignity cannot exist without Privacy. Both reside within the inalienable values of life, liberty and freedom which the Constitution has recognized.

The dilemma faced by policymakers in balancing an individual's right to privacy with national security issues has given birth to various tenets surrounding digital regulation, and its spillover effects can be seen in social behaviour, defence legislation, and multinational corporations. Historically, regulatory bodies and policymakers have struggled to strike a delicate balance between the right to privacy and national security, creating the need for more comprehensive regulation that safeguards both priorities. Privacy is an essential prerequisite to exercising individual freedom, and its erosion weakens the traditional constitutional foundations supporting democracy and good governance. Most democracies have incorporated the right to privacy as a basic constitutional right, however, this has often been undermined by legislation under the pretext of national security. Charters like the Digital Person Data Protection (DPDP) Act, 2023 in India and the EU's GDPR have attempted to provide data protection regulation mechanisms to balance individuals' right to protect their data but have also made provisions to process this data for lawful purposes. An example of this are surveillance programs like the Patriot Act post-9/11 in the US, and the NATGRID

[1] 4th year of 5-year Law course, Government Law College, Mumbai.

post-26/11 in India which have given the government and law enforcement agencies the power over wiretapping, email surveillance, and mobile device access. In contemporary times, governments have been demanding that tech companies create backdoors in their E2E encryption codes for them to access personal data in cases of potential national security breaches.

Data privacy regulations around the world hold private and public organizations responsible for safeguarding an individual's private information. However, law enforcement agencies have advocated for the need to retain data obtained through surveillance to combat fraud, corruption, crimes, and terrorism. Surveillance is both a national and an international issue since no government wants to fall behind in the intelligence race by limiting its power to conduct surveillance and gather data. The reasoning is that if one intelligence agency can handle and store significantly more data than other agencies, this gives the monopoly agency the power to weaponize that data by using it for digital espionage or diplomatic strong-arming against other nations. The promise of ensuring better security is not just a legitimate concern for the government, but also serves as an excellent electoral strategy.

Conversely, privacy activists argue that over-centralizing and concentrating intelligence and national security decisions into the hands of a select few can prove to be detrimental. The lack of elaborate accountability measures increases vulnerability to data breaches, and information misuse, and goes against the basic tenets of democracy that uphold decentralization of power. Moreover, the details we divulge about ourselves to other people are essential to our dignity and help us maintain control over who we are. Activists and international organizations like Human Rights Watch have asserted that the widespread practice of gathering data in the hopes that it might be useful later leaves people with little to no control over how they choose to define themselves to the government and other people.

Global surveillance agencies have argued that the disclosure of information obtained through surveillance and data-mining is not likely to threaten the privacy of law-abiding citizens, who have nothing to hide. Additionally, whatever minimal or moderate privacy interests law-abiding citizens may have in these particular strands of information are outweighed by the security interest in recognizing, investigating, and curtailing terrorist activities. This argument is flawed on multiple levels. Firstly, citizens are denied the ability to participate in how their data is collected, stored, and used. This data asymmetry imminently strains the relationship between the individual and the state. Secondly, when considering privacy from a utilitarian perspective, the nothing-to-hide[2] argument appears strong because privacy is sometimes seen as hiding unlawful activity. A more constructive way to approach the discussion is to view privacy as a family of issues. A tunnel vision approach regarding the right to privacy only as a means to conceal illegal activity can discourage people from engaging in lawful activity. The negative effect is that it narrows the spectrum of

[2] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 21-32 (2011)

opinions that can be said and discussed, and these opinions are usually at odds with state and populist goals. This further lessens the likelihood of dissent, which is a democracy's functioning valve.

When the privacy of an individual is weighed against the more utilitarian concepts of national security or 'the greater good,' it often results in the formation of ambiguous privacy regulations that allow the government to circumvent the very privacy standards the legislation seeks to uphold. The true question is not whether surveillance is necessary, but rather what kind of regulatory supervision and accountability measures should be enforced. Considering this, we must have strongly worded legislations that protect individual freedom while also allowing critical responses to national security threats. This necessitates the implementation of due process that eliminates arbitrary practices and amends how most agencies conduct their surveillance. The need of the hour is well-worded regulations that uphold the right to privacy while also giving room for exceptions which are limited in purpose, necessary and proportional to the aim, and accompanied by relevant procedural safeguards. Furthermore, we need a regulatory body that has the authority and mandate to impose privacy standards and monitor compliance.

Arbitrary regulations on digital privacy have a detrimental effect on businesses, especially those offering technology-based services. In contemporary times, the overzealousness of regulations on technical specifications might lead to additional challenges for the security programs of businesses. Companies must put in place certain security measures in order to comply with privacy regulations. Many companies only make minimal investments in security infrastructure to persuade auditors to affix a compliant badge to their lapel, but 'compliant' does not always equate to 'secure'. Organizations are compelled to tick all the boxes on a regulator's checklist, regardless of whether the tools serve the intended purpose. A viable solution to this would be to ease the stringent requirements that companies must comply with. Data protection regulations should move away from its objective of gaining access to information, and rather protect an individual's right to privacy as the name suggests. This in turn would protect people's rights and advance social justice while making it inherently conducive and convenient for businesses.