Page 966 - 975 **DOI:** *https://doij.org/10.10000/IJLMH.119176*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Privacy vs. Security: Balancing the Panopticon in this Digital Age

NIRBHAY AGGARWAL[1]

ABSTRACT

The Panopticon, Jeremy Bentham's circular prison cell concept, a theory based on the fact – 'One can be controlled, if enough fear of constant observation is created' which now has transcended its physical form to become an emblem of societal control, even though it is never realized. This abstract examines how the fundamental idea of this small-scale structure (panopticon)—the ability to continuously observe—has grown to be a key component of control.

A society comparable to Bentham's concept not restricted to prisons is now created by surveillance technology, such as CCTV cameras and digital monitoring through mobile applications, documents such as passports and financial records, which may not be physical but keep a constant check on an individual's activity and daily life, which was the sole essence of the Bentham's concept.

But this also brings a crucial question: Is this a part of freedom and independence, is constant surveillance on our daily life necessary for security, or does it compromise people's right to privacy?

The idea of the "invisible watchman" is remarkably applicable in the era of digital technology, showcasing our overdependence on technology and giving up on privacy under a social contract towards authorities. With each new technological development, the Panopticon's reach grows, as the technology would be controlled by a human being and the data collected could be stored in any part of the world. It may even include information one never expects to be shared and stored. Social media surveillance contributes to the further blurring of public and private domain boundaries.

While regulations are coming up to match the needs of the world, ensuring the data is safe and no one is misusing the information shared. The paper aims to evaluate the progress of technology and whether this is an authoritarian future of absolute control, or can strike a balance between security and privacy.

Keywords*: Privacy, Digital Security, Surveillance, Personal Liberty, Panopticons, Social Contract.*

[1] Author is a student at Lloyd Law College, Greater Noida, Uttar Pradesh, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The term Panopticon is derived from the Greek word *'Panopti',* which means 'all-seeing,' Philosophically, the concept was developed in the 18th century by British philosopher and jurist Jeremy Bentham (1742 – 1832) while traveling to Krichev in modern Belarus with his brother, Samuel. Bentham sketched out the concept of a panopticon of constant observation in prison from the ideas of his brother and continued to develop this theory[2]. He believed that this panopticon was perfect to ensure discipline in the prison cell, as this structure, if it came to life, would be in the form of a central observation system, where the cell would be open to a central tower. It will be built in such a way that only guards would be able to observe the inmates from the tower, while the prisoners would not even notice if anyone was in the tower or not. But this fear of constant watch through the tower will make sure that the inmates are behaving in the manner prescribed and the rules are being followed to the core. It is quite ironic that even though the guard may not necessarily observe a particular cell or inmate constantly. This seemed to be a great approach to ensure supervision as everyone would be self-disciplined, and according to him, the idea of this could be used for factories, asylums, hospitals, and schools[3] for supervision, though his idea of constructing this type of prison was never executed in real life and stayed as a hypothesis only.

Jeremy Bentham is also considered to be the father of the Analytical School of Jurisprudence, where sovereignty and command were central principles. He also believed that power should be visible and unverifiable. As he states, *"Liberty is the name of nothing positive"*[4] amounting to the idea that people only obey because they are accustomed to it, not necessarily due to its legitimacy. We learn what is right through fear of consequences, not inherent moral understanding. A 'right' does not exist without a law to enforce it. Combining the idea of constant surveillance would ensure law and order in the system, which is important to manage any society or group of people. Otherwise, people would be free to pursue any action they deem fit, which may lead to difficulties and inefficiency for the state and sovereign. In Indian jurisprudence, this principle is often examined in the context of reasonable restrictions on fundamental rights, particularly under Article 19 of the Indian Constitution.

[2] Sprigge, Timothy L. S.; Burns, J. H., eds. (2017). Correspondence of Jeremy Bentham, Volume 1: 1752 to 1776. UCL Press. ISBN 9781911576051.

[3] Gold, Joel; Gold, Ian (2015). Suspicious Minds: How Culture Shapes Madness. Simon and Schuster. p. 210. ISBN 9781439181560.

[4] Hart, H. L. A., 'The United States of America,' Essays on Bentham: Jurisprudence and Political Philosophy (Oxford, 1982; online edn. Oxford Academic, 22 Mar. 2012), https://doi.org/10.1093/acprof:oso/9780198254683.003.0004, accessed 6 May 2024.

 [ISSN 2581-5369]

The Supreme Court of India in the A.K. Gopalan case[5] upheld the state-imposed restrictions on individual liberty, emphasizing that '*no right is absolute and must be balanced against state interests.'* The Court even adopted a narrow interpretation of fundamental rights, holding that if the legislature properly enacted a law, it could restrict individual liberty. This was a landmark judgment impacting the security and privacy of citizens from the government. However, the government of India did not identify the importance of personal liberty for its citizens. It further established that the state could lawfully restrict individual freedoms for security reasons, even without requiring a test of reasonableness. This meant that the government had no accountability for their actions, and no citizen could enjoy privacy. This case showed a glimpse of how the government's concept of being 'all-seeing' is being implemented on the citizens of India by taking away their privacy.

However, Bentham's idea of continuous monitoring is not implemented directly here, but over the years, it has seen evolution, where the basic concept of keeping everyone under supervision so they can be controlled remains intact. The state, through various mechanisms, constantly keeps a check on all its citizens and monitors their activity closely. The state, through its various subsidiary authorities, might even act as an invisible observer, which goes unnoticed, where the citizens are unaware that they are under constant observation, just like a panopticon. Ironically, here citizens are not even aware of the same. CCTV cameras are just the beginning and a good fore-front, but what about cyber activities, Online payment gateways, and social media? Aren't these modes also part of surveillance, keeping a check on the daily activities conducted on their platform? Or are we living in a world where people do not even know who is keeping a watch on them? Is there any loophole that is unidentified, where privacy leaks in these situations do not curtail any individual's personal liberty?

II. CONTRADICTION WITH UTILITARIAN THEORY

Bentham gave a popular theory of Utility according to which "*The greatest happiness of the greatest number of people"*[6] As the majority has been controlled and overseen, most of them would not feel happy about it, which contradicts Jeremy Bentham's theory of utilitarianism, where he commits himself to the Principle of Utility:

By the principle of utility is meant the principle which approves or disapproves of every action whatsoever, according to the tendency which it appears to have to augment or diminish the

[5] A.K. Gopalan v. State of Madras (1950) AIR 27 SCR 88.

[6] Bentham himself used this phrase for the first time in his Preface to the Fragment but apparently did not use it again until 1820. Robert Shackleton, The Greatest Happiness of the Greatest Number: The History of Bentham's Phrase, 90 Studies on Voltaire and the Eighteenth Century 1461 (1972).

happiness of the party whose interest is in question: or, what is the same thing in other words, to promote or to oppose that happiness.[7]

But there are chances that many people are stuck for various reasons, due to which they are not getting maximum happiness. People constantly under surveillance or being monitored would not be a preferable condition for the citizens of the state. Even after raising concern in various cases and appealing that these actions can infringe upon the fundamental rights of people, the Court has emphasized that these rights are subjected to reasonable restrictions, especially when it concerns legitimate state interests, such as national security and public safety[8]. Although this case predates the recognition of privacy as a fundamental right, it also established that the state could lawfully restrict individual freedoms for security reasons. However, the Court also cautioned against intrusive surveillance that infringes upon fundamental rights, stating that: *"Surveillance may be intrusive and it may so seriously encroach on the privacy of a citizen as to infringe his fundamental right to personal liberty…. that cannot be permitted"*[9]. This judgment underscores the balance between the necessity of surveillance for public safety and the protection of individual privacy rights. Though the Courts have consistently advocated for a balanced approach, ensuring that surveillance measures are implemented within the bounds of the law and are subject to appropriate safeguards against abuse. The real question remains intact whether this constant surveillance provides maximum happiness to a maximum number of people.

Individual liberty should only be restricted to prevent harm to others and should be used for the greater good. The state should not curtail freedoms arbitrarily, as this leads to tyranny and long-term dissatisfaction in society. There are many contradictions over time, and different precedents are set, which widens the interpretation of this issue. But the law must ensure the greatest good for the greatest number, but not at the cost of fundamental rights.[10] Many believe that Bentham's Utilitarianism is also impartial in the sense that what matters is simply securing the maximum amount of pleasure for the maximum number of people; the theory does not give special preference regarding which people are supposed to have access to, or share in, that total pleasure.[11] Contradictions do always arise in these circumstances as the law is silent while

[7] J. Bentham, 'An Introduction to the Principles of Morals and Legislation,' in Utilitarianism and Other Essays, pp. 65.
[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[9] Malak Singh v. State of Punjab & Haryana, (1981) 1 SCC 420.
[10] John Stuart Mill (1859). On Liberty. In *Chapter VI of the Limits to the Authority of Society over the Individual* 4th Ed. Longman, Roberts, & Green Co. https://www.econlib.org/library/Mill/mlLbty.html?chapter_num=4#book-reader accessed on 03 March 2025.
[11] Dimmock, M., & Fisher, A. (2017). Utilitarianism. In *Ethics for A-Level* 1st ed., pp. 15. Open Book Publishers. http://www.jstor.org/stable/j.ctt1wc7r6j.5 accessed on 11 February 2025.

different doctrines and theories make it unclear which one should supersede and should be followed at the central level.

III. SYMBOL OF CONTROL

In the legal context, possession or authority over an object, person, or situation is established through symbolic means rather than direct physical control. This control was done through the enactment of various laws. Granting that out of a hundred law-abiding citizens, only one obeys the law from fear of its penalties, it does not follow that the penal system holds a corresponding insignificant place in the system of control.[12] Control is essential to maintain the conduct of citizens, which causes a fear of punishment. This control acts as a tool of supervision for the government and ensures security not only against the government but also within the state. However, when the line between protecting citizens and intruding on their privacy is touched, the process is reviewed so that people do not fear their leak of privacy. A judgment was passed in 2015[13] that reinforced that individuals should have control over their digital expression and security without government overreach, where Section 66A of the IT Act[14] was struck down for violating the freedom of speech[15] and privacy rights of the citizens.

Instances can be seen in daily life, how an individual's behaviour can be impacted through constant supervision, there are reality shows and games made on this subject[16] where participants live inside a house for days and are under surveillance twenty-four hours a day, for seven days, and anyone can just switch to the channel and enjoy. In the year 2023, they even introduced a 24x7 live option, where one can watch all the activities done by participants all day. This implies how the idea of the panopticon has taken a form of entertainment, where the participants are said to do anything abiding by the rules and staying non-violent amongst each other, but the fear of public image and opinions is always there, as every week a participant is eliminated from public vote according to their behavior throughout the week.

The show has proved the existence of the panopticon in the modern form, where it has turned into a business. The show is based on 'No-Privacy' as cameras are running all day, while the participants are made to perform tasks, given food, and sleep as per their behavior and performance, adapting the idea of jail panopticon from the work of Bentham. The idea of Michel Foucault of the 'invisible watchman' has now multiplied to various watchmen, where there is

[12] Ross, E. A. (1896). Social Control II. Law and Public Opinion. *American Journal of Sociology*, *1*(6), 753–770. http://www.jstor.org/stable/2761482.
[13] Shreya Singhal v. Union of India (2015) 5 SCC 1.
[14] Section 66A, The Information Technology Act, 2000 - Punishment for sending offensive messages through communication service, etc.
[15] Constitution of India, Art. 19 (1)
[16] Endemol Shine India. *Bigg Boss*, Viacom18.

no punishment involved, but various other benefits and purposes.

Take a red light with a traffic camera overhead. Many drivers stop, not necessarily because they respect traffic laws, but because of fear – fear of getting caught on camera and facing a ticket. This fear of surveillance can enforce desired behavior, prompting people to act according to societal or state expectations. However, is this the ideal motivator for following rules? This example raises a question about the underlying laws: should we obey them solely out of fear of punishment or because we understand their purpose and the benefits they bring to everyone? Ideally, a well-functioning society should foster a sense of civic responsibility, where people follow rules and guidelines because they recognize their value in creating a safe and orderly environment for everyone. However, people have argued against the same, giving reasoning that the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly the purpose of the establishment has been attained.[17] In the words of Philip Howard, Director of Research at the Oxford Internet Institute:

"We as citizens, have lost their first war of privacy"[18]

Today the blockchain technology, is often praised for its security and transparency. On the other hand, it is pertinent to mention that this information is not saved with the name of the person, but rather a blockchain wallet address which is linked to real-world identities, which can be traced back through an IP address if compromised. Any personal or sensitive information mistakenly recorded on its server cannot be deleted, which outright violates GDPR laws.[19] Companies and governments use blockchain forensic tools to maintain their surveillance by tracking transactions, uncovering user identities, analyzing spending behaviors, and much more.

IV. SECURITY WITHOUT ERODING PRIVACY IN THE DIGITAL AGE

"Our own information is being weaponized against us with military efficiency. Every day, billions of dollars change hands, and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded, and sold."[20]

The goal is to protect digital data from unauthorized access, simultaneously ensuring that the author of the data maintains full control over it, which is a difficult task at this age. Moreover,

[17] Nissenbaum, H. (n.d.). Privacy as contextual integrity: The panoptic view. Cornell Tech. pp. 34 Retrieved from https://nissenbaum.tech.cornell.edu/papers/panopticon.pdf. accessed on 11 February 2025.
[18] The Prezi version of this inaugural lecture, 'Is Social Media Killing Democracy,' can be accessed at: https://prezi.com/cxuukuoovaoc/is-social-media-killing-democracy/
[19] General Data Protection Regulation, 2016
[20] Tim Cook, CEO, Apple Inc.

this is due to the absence of strong legal and political reasons, which lack a structured law with strong enforcement with social contract theory between states, tech companies, and citizens. However, there is no strict procedure to secure 100% privacy of data in this digital age, while there are steps/measures to reduce the risk of authorized access and unnecessary surveillance:

1. *Reduce Digital Footprint* – Assuming nothing is safe once uploaded can be one of the key measures to reduce the risk of exposure. This can be attained if one reduces online exposure and does not rely solely on cybersecurity laws. Less personal information stored or shared on the internet will automatically mean fewer vulnerabilities.

   However, this may not reduce the surveillance by the authorities, but the exposure of the panopticon created would be much weaker than that to a person who exposed most of this information. Moreover, if the regulations are to be made strict, they should encourage organizations to collect only the data that is necessary for that specific purpose, which would increase the trust of the citizens to use that platform and reduce the risk of complaints against the organization in regards to privacy leak if the platform is compromised.
2. *Regular Audits & Compliance* – End-to-end encryption is one of the recent measures that have gained the confidence of customers over a platform to share their information. The sole idea of the information being kept between the platform and the customer reduces the panopticon vision through that platform, while the risk of being seen is still in place from other platforms.

   Keeping a constant check on private information as per the norms promised during the time taking the information keeping honest security audits and allowing users to review, edit, and delete their data in line with privacy policies. These platforms should publish reports on policy enforcement, breaches, and government data requests for the information stored. General Data Protection Regulation (GDPR) is a European Union regulation on information privacy in the EU and the European Economic Area, which is adopted to give rights to its citizens to erase the data. As per *Article 17*[21] of this regulation:

   1. *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*
      a) *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*

[21] Right to erasure ('right to be forgotten'), General Data Protection Regulation

b) *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*
c) *the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
d) *the personal data have been unlawfully processed;*
e) *the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
f) *the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).*

Similar measures to protect data should be adopted and should be followed to their core, this would ensure public trust and ensure the privacy of the data shared with the owner. Oversight mechanisms are thus the fundamental locking stone of the privacy-surveillance debate. Such institutions are designed to establish and monitor safeguards with the governments and act as bridges of public consent for surveillance/secrecy policies.[22] They also ensure that an abuse of the government's secrecy monopoly can be punished by the public through audience costs or electoral behavior.

V. CONCLUSION

Over the years, in the interpretation of status, the need of society, and modernization, major shifts in approach and judgments are seen not only in the world but also in reasons stated in judgment. Many precedents are been set, keeping in mind the needs of society and its impact on people for the foreseeable future. While A.K. Gopalan[23] upheld absolute legislative supremacy over personal liberty, later cases – especially the Maneka Gandhi[24] the case expanded the scope of Article 21[25], requiring that any restriction on personal liberty must be just, fair, and reasonable. This principle was reinforced in the K.S. Puttaswamy case[26], where

[22] Siobhan Gorman, "Reengineering Surveillance Oversight," Lawfare, September 6, 2017, https://www.lawfareblog.com/reengineering-surveillance-oversight.
[23] (1950) AIR 27, SCR 88.
[24] (1978) 1 SCC 248.
[25] Protection of life and personal liberty, Constitution of India.
[26] (2017) 10 SCC 1.

 [ISSN 2581-5369]

the Apex Court held that privacy is a fundamental right, but these rights are subject to reasonable restrictions if it comes in the interest of national security. While the no place that defines the scope and limitations of government using information and acting under the banner of 'National Security.' This gives them open access to any information and power to pass bills that may be as restricted as they want claiming it under the practise of national security.

The proposed Personal Data Protection Bill, now the Digital Personal Data Protection Act, of 2023, aims to regulate data collection and provide individuals with greater control over their data. The law is based on the idea that people should have the right to access, correct, and delete their data. Unchecked processing may have adverse implications for the privacy of individuals, which has been recognized as a fundamental right.[27] The Bill empowers the central government to notify certain data fiduciaries or classes of data fiduciaries, including startups, of certain obligations. This must be done with due regard to the volume and nature of personal data. One of the obligations that may be exempted is a notice of consent[28].

The question arises as to how the bill would ensure privacy and the security of citizens, as one without the other would only create supremacy of government over the state while the citizens stay under their supervision, causing an invisible panopticon in the country. [29]

This means there is always a scope of supervision beyond the knowledge of citizens by the centre; at times, it is with consent and at times implied under the banner of National Interest. The government may pass laws to protect privacy, but the security of that privacy is always a question. There are instances where the government has used the information beyond the scope of the consent given, be it for national security or mere supervision of certain groups of people. In this digital age, where countries are relying more on modern technology and the upliftment of it through recent judicial opinions[30] where the bench said *"If it is harmful. Do not use it, is it compulsory for you to use it?"* for the use of an AI tool named 'Deep Seek', where the petitioner questioned the possibility of the software being too sensitive, which may potentially misuse the data it stores, which cannot be controlled just by stopping its use, as these technology, typically updates itself every moment and stores data from any source on the internet, it has become quite difficult to keep the private data protected, due to which control over the internet, can easily breach anyone's security, this may help any central or state authorities to create an invisible

[27] Legislative Brief, The Digital Personal Data Protection Bill, 2023 https://prsindia.org/billtrack/prs-products/prs-legislative-brief-4181 accessed on 10 March 2025 accessed on 11 February 2025.
[28] *Supra*
[29] The Draft Personal Data Protection Bill, 2018; The Personal Data Protection Bill, 2019 and the Digital Personal Data Protection Bill, 2023 as introduced in Lok Sabha; Report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019; PRS.
[30] Bhavna Sharma v. Union of India & Ors. W.P.(C) 1762/2025

 [ISSN 2581-5369]

panopticon over the country and keep the country in unrealised fear and constant supervision. Given the above-mentioned circumstances and constant reliance on the internet, data protection through end-to-end encryption, passwords, etc., is still a subject in question. On one side any data that comes in any electronic form cannot be deleted permanently, which may help anyone to gain control of that data and understand the psyche of behavior, this may give him the power to manipulate through this constant surveillance over one's head, just like the working of the algorithms on our social media platform, which shows us advertisement of product which we desire or wants, which differs from the person sitting next to us. On the other hand, the government is trying to set up new regulations so that the data is always secure and no citizens fear their invasion of privacy. It is ironic that the government is using this information to keep a check on its citizens under the banner of national interest while creating laws to prevent it.

Today, the idea of a panopticon is totally different, which was not foreseen by anyone, especially Bentham, keeping not only the inmates but even normal citizens in constant fear. No way one can come out of this panopticon; the only measure left with us is to not rely on the internet completely and reduce the sharing of sensitive information unless necessary. In this world of consent leaks, safety is in our hands. The more we show or share our privacy, the more that person comes into the panopticon.

*****

 [ISSN 2581-5369]