Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Road to become a Surveillance state

Harsh Bansal[a]

[a]Rajiv Gandhi National University of Law, Patiala, India

Received 18 September 2021; *Accepted* 08 October 2021; *Published* 12 October 2021

No country can thrive if the citizens are not given their due rights. Our constitution provides some Fundamental rights to us, one of them is Article 21 which essentially provides a person, life, and liberty. As we all know, no provision of our constitution is static, rather the constitution is continuously evolving as the environment is evolving. New provisions and are added, and provisions are deleted as time passes. No one would have thought of the Right to Privacy being a fundamental right while the members were debating the constitution, but as time passed, it became essential to include the Right to Privacy as a fundamental right to protect its violation by the hands of state actors, private actors, and institutional actors. In the celebrated judgment of K.S. Puttuswamy vs, Union of India, Right to Privacy was included as a fundamental right under Article 21. But is this right absolute? The answer is negative as no fundamental right is absolute and unencumbered. Reasonable restrictions are placed to balance the needs of security of the state and the personal rights of citizens. In this article, we will discuss how India is on its way to becoming a surveillance state, and how it is affecting our international image.

Keywords: *state, privacy, surveillance.*

INTRODUCTION

"Liberty, when it begins to take root, is a plant of rapid growth"

- George Washington

WHAT'S A SURVEILLANCE STATE?

Mass surveillance is the complex monitoring of an entire, or a sizeable population of the country. It is generally carried out by the government, but can also be carried out by various agencies on behalf of the government. It is ostensibly undertaken to fight terrorism, protect the sovereignty and integrity of the country, and maintain peace and public order. Nowadays, it is being criticized for violating privacy, curtailing personal freedom, and being illegal under some jurisdictions. One important criticism is that it can lead to the development of a surveillance state where fundamental rights are infringed and political dissent (necessary for a thriving democracy) is undermined. Mass surveillance is considered a global issue, and some people say that the day is not far when states will be called 'GEOINT Singularity' in which artificial intelligence systems will monitor everything on earth. Many human rights groups and other concerned authorities have started creating awareness about the harms of expanding surveillance during the pandemic. In the guise of public order, mass surveillance has increased tremendously. It's a huge problem for normal citizens of the country because they can be denied some essential services if they refuse to give their personal information, and also face prosecution if they don't comply with the rules.

For example, all internet access in China is directly or indirectly controlled by the state. China is one of those countries which are on the track of becoming a surveillance state. The Chinese government is part of an active system of mass surveillance that violates human rights, the right to privacy, and freedom of expression. The mass surveillance system of China is called the Great Firewall of China,[1] it makes use of Deep Packet Inspection (DPI) technology,[2] to monitor and block access based on keyword detection. Private companies are answerable to the authorities to ensure that the banned messages are not circulated. According to an annual assessment of Comparitech,[3] Chinese citizens are the most monitored in the world. This surveillance network is being developed by China for a very long time with the help of the

[1] 'Great Firewall' (*Wikipedia*) <https://en.wikipedia.org/wiki/Great_Firewall> accessed 16 September 2021
[2] 'Deep Packet Inspection' (*Wikipedia*) <https://en.wikipedia.org/wiki/Deep_packet_inspection> accessed 16 September 2021
[3] Paul Bischoff, 'Which countries have the worst (and best) cybersecurity?' (*Comparitech*, 21 September 2021) <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/> accessed 21 September 2021

Golden Shield Project.[4] This project helped in the digitalization of law enforcement agencies with cameras fitted in every street and bots monitoring every corner. Chinese officials think that this can help them to anticipate threats to the regime, but the views of many western analysts and anecdotal evidence from history, and other social sciences prove that Chinese leaders' monitoring of their citizens will backfire.[5] If we go by history then the reaction of China to such an uprising will be violent and rapid which will confound western governments to decide whether to tolerate it, support protesters, or cut off diplomatic ties.

The world's largest democracy is also one of the largest surveillance states. Mass surveillance in India includes Surveillance, Telephone tapping, Open-source intelligence, Lawful interception, surveillance under Indian Telegraph Act, 1885,[6] etc. According to a Comparitech report,[7] when it comes to surveying its citizens, India ranks behind only Russia and China. Although in India right to privacy is a fundamental right, it is limited due to several factors like[8]:

1. Aadhaar database- the Aadhaar database has biometric data of around 1.25 billion people. It has been in the headlines in the past due to various data breaches,[9] and various petitions are still pending in the courts.

2. Data protection bill- It is yet to take effect and there isn't a data protection authority in place, meaning privacy protections are weak at present.

3. CCTVs – regulations relating to CCTVs are vague and open to interpretation which can lead to misuse and unlawful, extra-judicial surveying.[10]

---

[4] 'Golden Shield Project' (*Wikipedia*) <https://en.wikipedia.org/wiki/Golden_Shield_Project> accessed 16 September 2021
[5] *Ibid*
[6] Indian Telegraph Act 1885
[7] Sindhu Hariharan, 'India fails in privacy safeguards, says study' (*Comparitech*, 18 October 2019) <https://timesofindia.indiatimes.com/business/india-business/india-fails-in-privacy-safeguards-says-study/articleshow/71639597.cms> accessed 11 September 2021
[8] *Ibid*
[9] Yogesh Sapkale, 'Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast' (*Moneylife*, 19 February 2019) <https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html> accessed 11 September 2021

Surveillance can help in maintaining public order, security, integrity, and sovereignty of the state, but without any data protection law, the state can have access to private data, undermining the fundamental right to privacy of its population. Until 2017, it was unclear whether the right to privacy is a fundamental right or not, but after the celebrated judgment of K.S. Puttaswamy v Union of India,[11] right to privacy became a fundamental right under articles 14,[12] 19,[13] and 21[14] of the constitution of India. It was also held that it should not be infringed unless the same is necessary for protecting the sovereignty and integrity of the State. According to K.S. Puttaswamy, if the action of the State is arbitrary, the rights guaranteed under Article 14 of the Constitution would be infringed, and such an infringement would have to pass the test of reasonable restrictions under Article 19(2)[15] to survive constitutional and judicial scrutiny.

Article 12 of the Universal Declaration of Human Rights,[16] provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." In the famous case of Roman Zakharov v Russia,[17] the applicant contended against the mandatory practice of Russian telecom operators to install equipment's enabling search activities by law enforcement agencies, the court held that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such

[10] *Ibid*
[11] *K S Puttuswamy v Union of India* Writ Petition (Civil) No 494/2012
[12] Constitution of India, art 14
[13] Constitution of India, art 19
[14] Constitution of India, art 21
[15] Constitution of India, art 19(2)
[16] Universal Declaration of Human Rights 198, art 12
[17] 'Roman Zakharov v Russia' (*European Court of Human Rights*, December 2015) <https://hudoc.echr.coe.int/fre#%7B%22display%22:[2],%22itemid%22:[%22002-10793%22]%7D> accessed 12 September 2021

as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications will compromise the fundamental rights of the citizens.[18]

The Pegasus scandal[19] has once again brought into focus the issue of surveillance in India and the world. Pegasus is a type of malicious software which is developed by an Israeli firm that goes by the name of NSO group.[20] Once it's installed, it can gain unlimited access to all the data stored on the target's device along with all the pictures, videos, and WhatsApp messages. Therefore, it can be termed as one of the worst forms of attacks on an individual's privacy. It also infringes the right to free speech as journalists, human rights activists, and lawyers will not be able to share confidential information and messages. For surveillance, the Indian government mainly relies on the Indian Telegraph Act of 1885 and the Information Technology (IT) Act of 2000.[21] Indian constitution provides for the fundamental right to privacy and freedom of expression with certain reasonable restrictions in accordance with the doctrine of proportionality and rational nexus. The Indian Supreme Court clarified in the landmark case of PUCL v Union of India,[22] that the expression "public emergency" means the prevailing of a sudden condition affecting the people at large calling for immediate action, and the expression "public safety" means the state or condition of freedom from danger or risk for the people at large. The IT act and the telegraph act do not allow anyone, including the central government, to install spyware into mobile devices for unreasonable purposes and without compelling circumstances for which the criterion is provided in the statute itself.[23] We should understand that Pegasus spyware takes complete control of the target's mobile device which is technically hacking and is a criminal offense. It is punishable under various sections of the IT Act and the IPC[24]. To overcome all these problems and fulfill the requirements of natural justice and procedural safeguards, there should be a provision of judicial oversight because the

[18] *Ibid*
[19] Gordon Corera, 'Pegasus scandal: Are we all becoming unknowing spies?' (*BBC News*, 21 July 2021) <https://www.bbc.com/news/technology-57910355> accessed 14 September 2021
[20] 'Cyber Intelligence for Global Security and Stability' (*NSO Group*, 2021) <https://www.nsogroup.com/> accessed 9 October 2021
[21] Information Technology Act 2000
[22] *PUCL vs Union of India* AIR 1997 SC 568
[23] *Ibid*
[24] Indian Penal Code 1860

judiciary can decide whether the circumstances are reasonable enough to allow surveillance or not. Existing provisions regarding surveillance are weak and the proposed personal data protection legislation also gives wide exemptions to government authorities which again reinforces the need to have better and inclusive surveillance reforms.

PRIVACY DATA PROTECTION BILL

A brainchild of the K.S. Puttuswamy judgment named the Privacy Data Protection Bill (PDP)[25] was introduced by the Minister of Electronics and Information Technology (MeitY)[26] Ravi Shankar Prasad in Lok Sabha in 2019. It was a much needed and debated topic, so it was referred to a standing committee for microscopic scrutiny of the bill which would operationalize and acknowledge the privacy issues of the second biggest smartphone-using populace.[27] The Joint Parliamentary Committee (JPC),[28] is headed by BJP's Meenakshi Lekhi. The contention behind constituting this JPC was to strengthen the data protection laws while ensuring the privacy of the citizens. The bill sought to create a Data Protection Authority (DPA)[29] as a quasi-judicial authority to oversee the implementation of the act (when passed), adjudicate disputes which would be further appealable, provide machinery for the application of act (when passed), and prevent misuse of private data of individuals.

Some of the provisions of the act have led to condemnation and criticism because it provides wide discretionary power to government machinery to process and use data without the consent of the individual if the following circumstantial conditions are fulfilled: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency. Other points of criticism include the power of state actors to supply data to foreign actors with the explicit consent of the individual, but the state actors or fiduciaries can store that personal data within their databases, defeating the individual's right to privacy.

---

[25] Personal Data Protection Bill 2019
[26] 'Ministry of Electronics and Information Technology' (*meity.gov.in*) <https://www.meity.gov.in/> accessed 15 September 2021
[27] *Ibid*
[28] 'Joint Committee on the Personal Data Protection Bill, 2019' (*Parliament of India, Lok Sabha*, 2021) <http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1> accessed 15 September 2021
[29] Personal Data Protection Bill 2018

The state actors can host 'critical' data of an individual for which no criterion has been provided as to which type of data is critical or not. PDP allows fiduciaries/state actors to host and store data in (i) in the interest of the security of the state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to the commission of any cognizable offence (i.e. arrest without warrant) relating to the above matters. Processing of personal data[30] is also exempted from provisions of the Bill for certain other purposes such as (i) prevention, investigation, or prosecution of any offence, or (ii) personal, domestic, or (iii) journalistic purposes. Again, it contains some ambiguous and vague terms like Public order; personal, domestic usage; etc. Incorporation of these terms not just increases the horizon of state control but also exposes the personal data of an individual. The Hon'ble Supreme court in the case of Shreya Singhal vs. Union Of India[31] held that "a penal law is void for vagueness if it fails to define the criminal offence with sufficient definiteness. Ordinary people should be able to understand what conduct is prohibited and what is permitted. Also, those who administer the law must know what offence has been committed so that arbitrary and discriminatory enforcement of the law does not take place." These provisions (if incorporated) can open Pandora's box of petitions in various courts.

Another condemnable issue is that the DPA, which is said to be an independent body, is not very independent as the all the appointments are done by the central government, and the term is for 5 years.[32] Such control can lead to conflicting decisions as the central government would have indirect and disproportionate control. This is further violative of the doctrine of separation of powers which constitutes the basic structure and fabric of our constitution. Hon'ble Supreme court in the case of Madras Bar association[33] reaffirmed the doctrine of separation of power and said, "The Constitution has made demarcation, without drawing formal lines between the three organs— legislature, executive and judiciary. Separation of powers between three organs—the legislature, executive, and judiciary—is also nothing but a consequence of principles of equality enshrined in Article 14 of the Constitution of India.

[30] Bill 2019 (n 25)
[31] *Shreya Singhal v Union of India* Writ Petition (Criminal) No 167/2012
[32] *Ibid*
[33] *Madras Bar Association vs Union of India* Writ Petition (Civil) No 502/2021

Accordingly, breach of the separation of judicial power may amount to negation of equality under Article 14. Stated thus, legislation can be invalidated based on breach of the separation of powers since such breach is the negation of equality under Article 14 of the Constitution."

The infamous WhatsApp privacy policy, which created a ruckus doesn't apply to citizens living in the European region, why so? Let me tell you, the European Union (EU) has a comprehensive data protection law in place called the General Data Protection Regulation (GDPR),[34] this law prevents third-party intermediaries from sharing the personal data of users. What is the core difference between the PDP of India and the GDPR of the EU? We shall discuss some of them:

1. The territorial scope of GDPR is much narrower as it only allows entities of the union to process and store data with exceptions of goods and services, and behavior monitoring of individuals in EU member nations. Whereas, Indian PDP allows the processing of data that has been collected, disclosed, shared, or otherwise processed within the territory of India. It means that any foreign entity having residential offices in Indian territory can process and store data. It may expose the data of private individuals in India to foreign entities.
2. The basis for allowing intermediaries/fiduciaries/state actors to process/host/store data in India includes 'Reasonable Purposes' as may be specified by regulations, including for preventing or detecting unlawful activity, whistleblowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, the operation of search engines, or processing of publicly available personal data. The incorporation of such a clause further widens the contours of state control and narrows the contours of the right to privacy.
3. GDPR provides a right to data subjects (the person whose data is processed and stored) to not be subjected to automated decisions including profiling with some exceptions, and within those exceptions, the data fiduciary have the right to appeal the decision of

[34] 'Complete guide to GDPR compliance' (*gdpr.eu*) <https://gdpr.eu/> accessed 16 September 2021

being subjected to profiling. No such right is there in PDP. This makes the PDP less citizen-friendly.

4. GDPR necessitates the appointment of a representative to the Union if a foreign entity is processing the data in a large-scale manner, as social platforms like Facebook, Snapchat, etc. do. No such provision is there in India. This can make it difficult for India to assert its sovereign right.[35]

There are some other fundamental provisions that PDP possesses but GDPR doesn't. So, it can be said that PDP should be passed after resolving such loopholes to make it more citizen-inclusive and just in nature. Another point to be noted is that JPC scrutinization is taking a lot of time which will further increase as Meenakshi Lekhi (chairperson of JPC) became a minister.[36] Every day passing makes the data of millions of Indian users more exposed and vulnerable to misuse as evident by WhatsApp pushing down the throat its discriminative privacy policy.

NEW IT RULES

Ministry of Electronics and Information technology recently introduced new rules for the application of the Information technology act, 2000 (herein referred to as' IT act') as per the power conferred by sub-section 1[37] and 2[38] of section 87 of the IT act. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021,[39] provides a framework and a code of conduct to be followed by IT intermediaries while discharging their duties. These rules came under criticism for their wide discretionary powers and surveillance apparatus which inhibit independent functioning and having a chilling effect on the privacy of an individual. But, another important lacuna to be noted is that these rules go against the provisions of their parent act (IT act, 2000) and the Shreya Singhal judgment.[40] As per rules

[35] *Ibid*
[36] Joint Committee (n 28)
[37] Information Technology Act 2000, s 87(1)
[38] Information Technology Act 2000, s 87(2)
[39] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[40] *Shreya Singhal* (n 31)

3(b)[41] and 3(d)[42], the intermediaries have voluntary and discretionary power to take down any content upon any complaints received by private individuals/entities. Rule 3(d) further provides that "the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a **voluntary basis**, or on the **basis of grievances received** under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a)[43] or (b)[44] of sub-section (2) of section 79 of the Act." This is a blatant disregard of the Supreme court's judgment in Shreya Singhal's case, in which it was held that intermediaries cannot decide if a request is legitimate or not. For the same reason, Rule 3(1)(d)[45] also goes beyond its parent legislation, i.e., Section 87 of the IT Act, 2000,[46] which prescribes that the rules may be made in furtherance of Section 79(3) of the IT Act, 2000.[47] However, the said rule is completely beyond the scope of Section 79(3) of the IT Act 2000, as it permits a private intermediary to remove access to information voluntarily or as per a complaint made by a private individual, which renders it illegal and unconstitutional given the judgment by a constitutional bench in Shreya Singhal's case.[48] The Hon'ble Supreme Court of India in the case of Sarbananda Sonowal[49] held that "any subordinate legislation brought in to defeat the mandamus issued by the Hon'ble Supreme Court, without an amendment to the parent legislation, is arbitrary and liable to be struck down as unconstitutional".

These rules also defeat the K.S. Puttuswamy judgment,[50] as the rules do not provide for the basis and mechanism by which the intermediaries can voluntarily take action, without any surveillance of the users. In the said judgment, the Hon'ble Supreme Court carved out various forms of privacy, such as communicational privacy, behavioral privacy, online privacy among others which are completely violated as the intermediaries are empowered to voluntarily act

[41] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3(b)
[42] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3(d)
[43] Information technology Act 2000, s 79(2)(a)
[44] Information technology Act 2000, s 79(2)(b)
[45] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3(1)(d)
[46] Information Technology Act 2000, s 87
[47] Information Technology Act 2000, s 79(3)
[48] *Shreya Singhal* (n 31)
[49] *Sarbananda Sonowal v Union of India* Writ Petition (civil) 131/2000
[50] *K S Puttuswamy* (n 11)

and remove access to information and/or block access to accounts. Communications over WhatsApp or Telegram are end-to-end encrypted, which means that only the two users communicating with each other can view the messages and no other third party has access to the same. To voluntarily act under the Impugned Rules, WhatsApp or Telegram is empowered to constantly watch all communications taking place on the platform and take down the iron and steel wall of privacy. In fact, the intermediaries are constantly under threat of criminal liability if they do not breach the privacy of the users to track the data, the information being exchanged, and identify the first originator.

Rules 3(1)(b)(viii)[51] requires the intermediaries to remove information that threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting other nation. In the said rules, no definition or constitutive interpretation has been provided to identify which information can be termed as capable of inciting violence or disturb public order, or for that matter, what even constitutes public order? Suppose, if an oversensitive person gets offended by something which is against his personal thoughts and ideologies, and complains the intermediary to take down the information, which the intermediary is obligated to do under the provisions, defeats the very spirit of fundamental right to free speech and expression, and also does not pass the test of rational nexus and proportionality envisaged by various judgments, and recently the Anuradha Bhasin judgment.[52] The said judgment recognized the freedom of speech and expression even on the internet as a fundamental right, which is only curtailable by article 19(2), which provides for reasonable restrictions which only the state could apply, and not a private intermediary. Even though fundamental rights cannot be strictly enforced against private entities, the State cannot create a mechanism by way of a positive action allowing private entities to violate fundamental rights and delegate their duties.[53]

[51] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3(1)(b)(viii)
[52] *Anuradha Bhasin v Union of India* Writ Petition (Civil) No 1031/2019
[53] *Ibid*

It is pertinent to note that the procedure for disposing of a complaint prescribed by the rules contains no provision for the author/originator of the information to be heard before the information is taken down, depriving him of his fundamental rights and natural right of being heard. The procedure by which such complaints ought to be decided has also not been prescribed, once again giving deep and pervasive powers to the private intermediaries to control the private and personal lives of the citizens who use such platforms. The complaint made will be decided without holding a trial or any procedure by which the author/originator of the information can defend his actions. It is evident that these rules are not protective, but are akin to censorship, and further adds to the contemptible journey of India in becoming a surveillance state.[54]

INTERNET SHUTDOWNS

In 2020, India became the country with the highest number of internet shutdowns. in 2019 also India was at the top. As per a report,[55] India has topped the list of 29 countries that disrupted internet access followed by middle eastern countries and some parts of Africa with 109 out of 155 total global shutdowns. It is alleged that some shutdowns are imposed to suppress protests and to crack down on political rivals and dissidents. Due to the COVID-19 pandemic, almost everything which was done offline was forced to shift online, and in such a scenario, intentional disruption of internet services can have a very negative effect as it disrupts education, business activities, and access to medicines and life-saving drugs. There have been reports that show an increase in the incidence of internet shutdowns to thwart protests and suppress dissent. According to the laws of India, authorities can ask the telecom companies to disrupt internet access and also to take down certain sites, but many citizens are against these laws as they violate their right to freedom of speech. Indian authorities have been continuously using the disruption of internet services as a tool to quell demonstrations.

---

[54] *Ibid*

[55] 'India's Shutdown Numbers' (*Internet Shutdowns*, 2021) <https://internetshutdowns.in/> accessed 17 September 2021

In August 2019, India instituted a perpetual and punitive internet shutdown in Jammu and Kashmir.[56] Although, there have been earlier shutdowns, this time it was perpetual and overbearing. This internet shutdown was imposed before the abrogation of article 370 during which people had access to only 2G services. People were denied access to high-speed internet for nearly two years, due to which, students' overall ability was affected, especially during the pandemic. With 2G services, students cannot join video classes, so they were forced to join audio classes which were also not free from technical issues and glitches. In February 2021, 4G internet services were finally restored to normalcy in Jammu and Kashmir.[57] These internet lockdowns have caused widespread alienation and a sense of abandonment in the people of Jammu and Kashmir. The government claimed that the internet shutdown was imposed due to security reasons as the government considers social media and other online platforms as the primary drivers of militancy.[58] Despite such stringent restrictions, at least 203 fatalities have been reported from militant activities between 1 January and 22 July 2020, including 17 civilians, 34 security personnel, and 152 militants. The region also saw 223 terror-related incidents over the same period.[59] The official reasons for shutting down the internet were legitimate, but shutting down the internet also hampers the movement and communication of citizens of the state. Despite the opposition from retired military officers, journalists, human rights organizations, and the general public, the government continued its longest-ever internet shutdown. Internet shutdowns have mainly focused on economic and political bearings while neglecting consequences on the educational sector.

In January 2020, the supreme court of India got an opportunity to decide on the longest internet shutdown in the case of Anuradha Bhasin v. Union of India,[60] (hereinafter 'Anuradha Bhasin'). According to this judgment, there should be a balance between the fundamental right

[56] 'India's Shutdown Numbers' (*Internet Shutdowns*, 2020) <https://internetshutdowns.in/> accessed 16 September 2021
[57] Express Web Desk, 'Restoration of internet services in Jammu and Kashmir: A timeline' (*The Indian Express*, 5 February 2021) <https://indianexpress.com/article/india/jk-4g-internet-mobile-timeline-7176408/> accessed 15 September 2021
[58] *Ibid*
[59] Khalid Shah, 'How the world's longest internet shutdown has failed to counter extremism in Kashmir' (*Observer Research Foundation*, 22 August 2020) <https://www.orfonline.org/expert-speak/how-the-worlds-longest-internet-shutdown-has-failed-to-counter-extremism-in-kashmir/> accessed 15 September 2021
[60] *Anuradha Bhasin* (n 52)

of citizens and the security of the country. The Supreme Court of India ruled that an undefined restriction of internet services would be illegal, and orders for internet shutdown must satisfy the tests of necessity and proportionality.

Proportionality is a principle in which the court is concerned with the process or method in which one has arranged his priorities. The doctrine of proportionality involves a 'balancing test' and a 'necessity test'. Balancing test permits the scrutiny of onerous penalties or infringement of rights whereas the necessity test requires infringement of fundamental rights to the least restrictive alternative. In simpler words, it means that whether the method employed to achieve the particular objective is justified by that objective's potential benefits or not. In addition to the rules concerning the suspension of internet services, the SC stressed a periodic review and non-permanence of such orders. Most importantly, the Court held that the "freedom of speech and expression and the freedom to practice any profession or carry on any trade, business or occupation over the medium of internet enjoys constitutional protection under Article 19(1)(a)[61] and 19(1)(g)[62] of the Constitution of India." The court did not remove the restrictions on the internet and the movement of the citizens; however, the judgment widened the interpretation of freedom of speech and expression by including the right to access the internet as a fundamental right.

Internet shutdowns are not limited to Jammu and Kashmir only, the West Bengal Board of Secondary Education and the state government's Home Department previously introduced a curfew-style internet blackout during the Madhyamik (secondary school) examinations, cutting off internet access every day during certain hours.[63] This internet curfew lasted for more than nine days. according to a report on access now, a total of 28 lockdowns were imposed. People were forced to live without the internet as broadband and internet connectivity were disturbed.[64] Recently, the Haryana government ordered an internet

[61] Constitution of India, art 19(1)(a)
[62] Constitution of India, art 19(1)(g)
[63] The Wire Staff, 'Over 100 Instances of Internet Shutdown in India in 2020, Says New Report' (*The Wire*, 4 March 2021) <https://thewire.in/tech/over-100-instances-of-internet-shutdown-in-india-in-2020-says-new-report> accessed 15 September 2021
[64] *Ibid*

shutdown in Karnal district to quell farmer protests.[65] It said that the suspension of mobile Internet services was ordered to stop the spread of misinformation and rumors through social media platforms such as WhatsApp, Facebook, and Twitter on mobile phones.

CONCLUSION

Unfortunately, the biggest democracy in the world is straying away from its core democratic principles and the fundamental rights which our constitution prescribes to us. As per the Comparitech survey,[66] India ranks third-worst out of 47 countries in terms of privacy and surveillance, only behind China and Russia. India is not in the 128 out of 194 countries,[67] that have devised legislation to protect privacy and data. India ranked 142 out of 180 countries in World Press Freedom Index.[68] India ranked 111 out of 162 countries on Human Freedom Index.[69] These surveys paint a grim picture of the deteriorating international image of India in international forums. To rectify the mistakes and purify our image, the authorities should focus on putting up an all-encompassing, citizen-friendly, least-intrusive Personal Data Protection Bill and get itself eliminated from the race of becoming a surveillance state.[70]

---

[65] Staff, 'Internet shutdown in five Haryana districts ahead of farmers' protest' (*The Tribune*, 7 September 2021) <https://www.tribuneindia.com/news/haryana/internet-shutdown-in-five-haryana-districts-ahead-of-farmers-protest-307753> accessed 15 September 2021

[66] Bischoff (n 3)

[67] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 15 September 2021

[68] '2021 World Press Freedom Index' (*Reporters Without Borders*, 2021) <https://rsf.org/en/ranking> accessed 17 September 2021

[69] Ian Vasquez & Fred McMahon, 'Human Freedom Index' (*CATO Institute*, 2021) <https://www.cato.org/human-freedom-index/2020> accessed 17 September 2021

[70] *Ibid*