**International Research Journal of Commerce and Law**
Volume 12 Issue 06, June 2024 ISSN: 2349-705X Impact Factor: 8.843
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

# Digital Surveillance and the Right to Peaceful Assembly

**Praveen kumar, Research Scholar**
University Department of law
T.M.B.University, Bhagalpur

**Abstract**

*The liberty to meet peacefully is a critical prerequisite of the democracy and allows the citizens to show their dissatisfaction, struggle to social change and participate in group political action. Nonetheless, digital surveillance devices, such as facial scanning, cell phone surveillance, biometrics identification and social media surveillance, have also raised grave concerns as far as the erosion of the right is concerned. So despite the governments being inclined to defend surveillance by their security concerns, counterterrorism and the preservation of order, the surveillance by the governments is rather restrictive, therefore, sending chilling effect to civic life, and also discouraging the people to protest. The paper has examined how digital surveillance is converging with the right to assemble peacefully, through the international standards of human rights, standards in the region and national jurisprudence. It draws on the example of Hong Kong, the United States, India and Europe in order to evaluate how the various legal systems are struggling to reconcile the demands of security and the democratic rights. The work brings forward an argumentation of how unregulated surveillance poses a threat to the privacy and the process of democracy. It identifies the need of the law to provide protection, independent monitoring and technology governance (in the form of rights). The defence of the right to assembly, in the digital age, along with being extremely important to the health of democracy also needs defence of the arbitrary state power.*

***Keywords:*** *Digital Surveillance · Right to Peaceful Assembly · Facial Recognition Technology · Privacy and Human Rights · Chilling Effect*

## I. Introduction

The digital era has also been characterised by an increase in surveillance systems, including facial recognition system, phone tracking, biometric identification and algorithmic monitoring of social media sites. Whilst governments have always provided reasons that the tools are needed to ensure that there is security and peace in the country, there have also been serious apprehensions over the declining freedom of civil liberties, and most importantly freedom of peaceful assembly with the use of the tools.

### Importance of Right to Peaceful Assembly

Peaceful gathering is one of the foundations of the democratic states, and it gives citizens the right to express dissent, organise to bring about social or political change and to affect the processes of governance. Guaranteed by the international human rights documents like Article 20 of the Universal Declaration of Human Rights (UDHR) and Article 21 of the International Covenant of Civil and Political Rights (ICCPR) as well as national constitutions, e.g. Article 19(1)(b) of the Indian constitution and the First Amendment of the US constitution, this right is the foundation of the participatory democracy.

**Research Problem**

The central question concerns the need to reconcile the interests of the state in security, counter-terrorism and upholding the order in society with their right to freely congregate without fear of being spied on by the state. The conflict becomes critical when surveillance activities are unwarranted, disproportional or discriminatory and thus replaces justifiable protests and interferes with freedoms of democracy.

**Objectives of the Paper**

1. To explore the extent and constraints of the right to peaceful assembly in the digital surveillance context.
2. To analyse the ways in which different legal systems deal with the tensions between surveillance and the right to assemble.
3. To assess case studies with the real-world implications of digital monitoring on civic participation.
4. To recommend legal and policy measures that will guarantee democratic guarantees in the digital age

**Methodology**

It is a doctrinal and analytical paper, which examines international conventions, provisions in the constitution and judicial interpretation. It further relies on similar case studies across several jurisdictions (India, United States, Hong Kong and Europe), to indicate practical implications. Also, the study utilizes the secondary information sources, such as reports, scholarly commentaries and policy papers to critically evaluate how far security requirements override basic liberties.

**1. Peaceful Assembly as a Fundamental Right**

**1.1 International Perspective**

Peaceful assembly is one of the fundamental democratic liberties that the international law recognizes. According to article 20 of the universal declaration of human rights (1948), the freedom of assembly and association of individuals is a right granted by the UN (United Nations, 1948). Likewise, Article 21 in the International Covenant on Civil and Political Rights (1966) secures this right, but in cases where it is limited, it must be lawful, necessary and proportionate to legitimate purposes such as national security, civil safety or the security of the rights of others (UN General Assembly, 1966). The European Convention on Human Rights (Article 11) grants similar safeguards with the states having to fulfill very stringent legality and proportionality criteria prior to any such interference (Council of Europe, 1950). Moreover, in a General Comment No. 37 (2020), the UN Human Rights Committee notes that digital surveillance of assemblies is a novel threat to democratic freedoms, and should not be employed to intimidate or discourage participation (UN Human Rights Committee, 2020).

**1.2 National Perspective**

The rights to assemble are also preserved by domestic constitutional systems. Article 19(1)(b) of the Constitution in India provides a right to assemble peacefully and without arms but Article 19(3) allows a reasonable restriction in the interests of sovereign or order (Government of India, 1950). The right to assemble the people in a peaceful way is specifically protected in the First Amendment in the United States,

where it is alongside speech, press and religion freedoms (U.S. Const. amend.). I, 1791). Equally, freedom of association and assembly is acknowledged in the Charter of Fundamental Rights of the European Union (2000) (Article 12), an important right in both conventional and online civic participation (European Union, 2000). These clauses emphasize universal acknowledgement of the right to assembly and give room to legal discussions regarding the scope of the restrictions that can be made.

## 2. Digital Surveillance Defined

### 2.1 Tools and Methods

Digital surveillance can be described as the utilization of high-end technological devices to track individuals, groups or activities. Some of these tools are facial recognition technologies, which are frequently used at large-scale events to identify participants (Bedoya, 2019); mobile phone tracking, where the whereabouts of protestors are tracked using the location information (Rahman, 2021); and drones, which enable protesters to be observed in the air (Finn and Wright, 2012). Governments also do online surveillance, social media and communications are scanned to identify protest-related activity (Gill, Redeker, and Gasser, 2019). Furthermore, biometric databases are starting to associate identities with national records, which is concerning in the long term because of retaliatory or profiling (Greenleaf, 2018).

### 2.2 Evolution from Physical to Digital Surveillance

Traditionally, the surveillance of assemblies was based on the visible means like the presence of police, photography, and informants. With the introduction of digital technologies, though, surveillance is more widespread, less apparent and data-driven. Digital surveillance enables states to track protestors prior to, in the middle of, and after an assembly, and leaves behind a digital trail that can be utilized to profile or otherwise retaliate against protestors (Lyon, 2018; Farraj, 2020). This change shifts the priority between the state security interests and individual freedom because the surveillance power is growing, which threatens to weaken privacy and democracy engagement (Zuboff, 2019).

## III. The Intersection of Digital Surveillance and Assembly Rights

### 1. Impact on Democratic Participation

The surveillance in the digital space sends a chilling effect on the propensity of the citizens of the country to exercise their right to assemble. People usually do not attend a demonstration when they know that facial recognition cameras, phone tracking, or social media monitoring can be directed at them, even when such events are legal (Penney, 2017). This consciousness breeds the fear of retaliation, such as the threats of being harassed by the police, job revenge, or political victimization (Gill et al., 2019). In the long term, these practices result in self-censorship, i.e. people do not want to express their dissent, do not want to engage in civic activities in order to take care of themselves (Lyon, 2018). These are immediate effects undermining the democratic participation based on the open, collective, and fearless involvement in the public life.

### 2. State Justifications

Governments tend to justify surveillance activities by citing reasons of national security, violence prevention and preservation of order in the society. When it comes to a scenario where there is a threat of

terrorism or a civil conflict, surveillance is introduced as a preventive measure that can help the government identify hazards and safeguard its population (Donohue, 2016). In the international human rights law, however, the limitation to assembly should be in accordance with the necessity and proportionality tests (UN Human Rights Committee, 2020). This implies that minimal interference is to be used, and it is not in keeping with democracy to monitor protestors indiscriminately or blanketly. Surveillance without justified reasons and proper control is likely to turn into an instrument of oppression instead of safety.

### 3. Risks and Concerns

However, regardless of the state arguments, the risks of digital surveillance are high. Arbitrary minorities, activists, and opposition group targeting can be one of the most worrisome as it may strengthen other inequalities and silencer critical voices (Farraj, 2020). The lack of transparency and accountability of the use of surveillance technologies is also a matter of concern. People are not often aware of the type of data collected, its duration, and the persons who can access it (Bedoya, 2019). Lastly, the abuse of data and its future impacts are also very grave. After being collected, the information can be used to profile, manipulate politically, or even sold (Zuboff, 2019). These dangers show that there is an essential necessity of strong safeguards so that the digital surveillance would not compromise the democratic freedoms.

## IV. Case Studies

### 1. Hong Kong Protests (2019–2020): CCTV and Mobile Phone Monitoring

In the 20192020 pro-democracy protests in Hong Kong, the government put in place vast surveillance technology, such as CCTV and mobile phone tracking systems, as well as facial recognition systems. Protestors have claimed that the government was using geolocation features to track those people in certain locations, and CCTVs that read faceprints were placed in key population centers (Mozur, 2019). As a reaction, numerous protesters embraced counter-measures (e.g., putting on masks, not using electronic payments, or turning off mobile phones), so that they became less traceable (Kuo, 2020). The mass surveillance did not only create an issue of breach of privacy but also created a deterrent effect, as people felt discouraged to engage because of the fear of being caught in the long-term.

### 2. United States (BLM Movement, 2020): Surveillance: Drones and Facial Recognition Surveillance.

The 2020 Black Lives Matter (BLM) protests in the United States that resulted due to the killing of George Floyd demonstrated that the government was dependent on the most sophisticated surveillance technologies. The federal authorities, such as the Department of Homeland Security were watching the participants with the help of aerial drones, facial recognition, and social media monitoring (Stanley, 2020). Spying was reportedly spread to reporters and legal observers and the violation of the First and Fourth Amendments brought up the question of constitutionality (Guariglia, 2020). The opponents believed that these practises were spine-chilling on the freedom of speech and assembly especially in communities where the community was already facing disproportionate policing.

### 3. India (CAA/NRC Protests): social media monitoring and Biometric data.

The social media surveillance and biometric identification system was highly applied in the protests against the Citizenship Amendment Act (CAA) and National Register of Citizens (NRC) in India. Police were reported to be able to follow the chats of WhatsApp, Facebook pages and Twitter accounts to monitor the

organisers and activists of the protests (Bhat, 2020). It has even gone to the extent of the facial recognition systems being connected to the databases built on Aadhaar being scanned in protest sites in Delhi to identify protesters (Jain, 2020). Not only did these practises create the issue of legal concern in relation to the light of Article 19(1)(b) of the Indian Constitution, but also created certain tension between the practises and the idea of privacy as a fundamental right of the Supreme Court, as was stipulated in the Puttaswamy case (2017). The critics cautioned that the unregulated monitoring of the protests would most probably stifle the dissent and the minority rights.

**4. European Union: Data Protection Structures v. Rights of Public Assembly.**

The situation is different in Europe Union where the system of data protection is more protective to the citizens. According to the General Data Protection Regulation ( GDPR, 2018), there are strict boundaries of the collection and to the processing of the personal data, including the data obtained by surveillance technologies (European Parliament, 2018). In spite of the fact that some of the states within the EU attempted CCTV and digital surveillance in assemblies, both are often doubted in the GDPR and the European Convention on Human Rights (Article 11) (Buttarelli, 2019). Nevertheless, the issue of the extent to which surveillance is required to guarantee the safety of the population and the freedom of assembly remains debatable in the context of the enhanced implementation of the said technologies as predictive policing and AI-powered analytics.

**V. Legal and Human Rights Analysis**

**1. International Standards**

**Children under arrest in the US Courts.**

On many occasions, the UN Human Rights Council (UNHRC) has pointed out that no one must be oppressed through peaceful protest by means of digital surveillance. In the recent resolution on the Right to Privacy in the Digital Age (2014), the Council has emphasised that the surveillance must be performed within the framework of the above principles of legality, necessity, and proportionality, and must also have proper means of control (UNHRC, 2014). The Council has also proposed states to explain how they will proceed with the surveillance and develop mechanisms that would ensure that the information of the citizens is not abused.

**General Comment No. 37 on ICCPR**

Article 21 of the ICCPR provides that people have a right to assemble peacefully, which has a direct interpretation with reference to the General Comment No. 37 (2020) of the UN Human Rights Committee. The Comment acknowledges the more active use of digital surveillance, facial recognition and phone tracking, and provides a reminder that these actions may demoralise assemblies attendance. It also explains that surveillance cannot be an intimidation and harassment instrument to the subjects and any restriction should pass the legality, legitimate aim, necessity, and proportionality test (UNHRC, 2020).

## 2. Regional Frameworks

### European Court of Human Rights Rulings

Through Article 11 of the European Convention on Human Rights, the ECtHR has been in a position to develop a jurisprudence on the right to the peaceful assembly. In Kudrevičius v. The Court concluded that limitations were supposed to be aimed at a pressing social need, and need to be commensurate to purposes (Lithuania, 2015). In Big Brother Watch v. According to the Court (United Kingdom, 2018), mass and indiscriminate surveillance systems are most likely to undermine the principles of democracy that the Convention is meant to protect (ECtHR, 2018). These rulings support that the level of surveillance must remain at the bare minimum in order not to cause a chilling effect of the protests.

### Jurisprudence International Human Rights Inter-American.

Even the Inter-American Court of Human Rights (IACtHR) has found the chilling effect of surveillance on the right to assemble. It has pointed out that surveillance must not be arbitrary and discriminating, and must be rich in security against abuse. Surveillance can equally be disproportionately directed against vulnerable populations, activists, and in a disproportionate way, but it may be harmful to freedom of expression and the right to organise in peace, as was highlighted in its Advisory Opinion OC-23/17.

## 3. National Jurisprudence

### India: Jurisprudence and Article 19(1)(b).

Article 19(1) of the Constitution of India also ensures the right to assemble peaceably with reasonable limitations provided by Article 19(3). This right has been affected by the Supreme Court in its historic ruling in Justice K.S. Puttaswamy v. UNEP (2017) which considered privacy as a fundamental right. The Court found that online surveillance, which is one of the constraints to privacy, must be placed under in question of legality, necessity, and proportionality (Bhatia, 2017). The framework directly affects the manner in which the surveillance of assemblies is to be considered in the Indian law.

### The first and fourth Amendment controversies in the United States.

Both the First (freedom of speech and assembly) and the Fourth Amendment (protection against unreasonable searches and seizures) of the United States are at play in the surveillance of the protests. The courts have issued a warning that the government is not allowed to use surveillance to gather information on individuals due to his or her political opinion (ACLU, 2020). However, the Black Lives Matter events have raised the issue of whether or not the current constitutional norms are adequate in the context of the digital era as a result of drone usage, facial recognition, and online surveillance (Stanley, 2020).

### United Kingdom: Surveillance Legal Right and Legal Right of Protest.

The major law-givers of the surveillance in the UK are Investigatory Powers Act 2016 and Regulation of Investigatory Powers Act 2000. Such structures have been denounced because they provide broad powers to the authorities when they possess cheques and balances of the judiciary and parliament. The reasons of the civil liberties groups are that this legislation will enable the government to over monitor protests, which could be in breach of Article 11 of ECHR that has been incorporated into the local law through the Human

Rights Act 1998 (Liberty, 2019). This is the conflict to show the unresolved issue of the state security authorities and the rights of the assembly.

## VI. Ethical and Socio-Political Dimensions

### The Privacy vs. Collective Security debate.

One of the oldest ethical concerns that digital surveillance in group presents is a balance between personal privacy and security in the group. States tend to argue that monitoring must be done to prevent violence, terrorism, or danger to the order. However, this defence carries the risk of what is referred to as the morally justified repression of individual agency and civil liberties by intrusive groups of practises (Solove, 2021). The ethical theory states that security, as a good goal, should not be pursued by compromising the fundamental rights such as privacy and the right to assemble, which are equally valuable to democratic security (Lyon, 2018). Proportionality is hence a matter of degree: just how much excessive surveillance is not necessarily a virtue but at what stage does it begin to suffocate the dissent rather than guaranteeing the safety of the society as a whole?

### Inequality and discrimination in Surveillance Practises.

Equity and fairness are other problems that digital surveillance raises. It has also been established that the non-dominant ones, such as ethnic minorities, immigrants, or political dissidents, are the targeted groups of the surveillance systems (Eubanks, 2018). The algorithms dealing with facial recognition, including that one, have been claimed to be race and gender biassed and, therefore, have a higher error rate with people of colour and women (Buolamwini and Gebru, 2018). Such discrimination not only goes against the human rights, but improves the social inequality since the vulnerable groups are the ones, who must face the encroaching surveillance**.**

### Role of Technology Companies ( Private Actors).

The other defining dimension which is critical is the role of the private technology companies. Facial recognition software, mobile tracking apps, and AI-based analytics are some of the state surveillance tools, which are developed and sold by the private companies. This presents certain ethical issues of accountability whereby the private actors have a higher chance of operating without much visibility, and beyond the formal human rights systems (Feldstein, 2021). Even the privatisation of the very process of surveillance undermines the distinction between the state and the corporate authority and, hence, makes it even more challenging to control the accumulation, storage and spread of the information.

### Civil Society Resistance

The identity of the civil society organisations is extremely important in questioning the improvement of the digital surveillance. Lighting, policy lobbying, and campaigns are some of the tactics applied by the advocacy groups, digital rights activists, and non-governmental organisations as a way of holding states and corporations accountable (Gill et al., 2019). The demonstrations in the United States such as the Stop Facial Recognition Campaign and the Privacy International in Europe have demanded that some of the technologies should be regulated and prohibited entirely. Such a step shows how the grassroots activism fit in the protection of the civic space so that the technological development would not affect democracy but rather would strengthen the latter.

## VII. Recommendations and Way Forward

### 1. Laws to restrict excessive use of surveillance.

The laws should be changed to make sure that the digital surveillance will not jeopardise the freedom of the democratic process. The governments should also formulate laws that set final limits and boundaries of the technologies employed in surveillance so that it is only employed when it is necessary, and to the extent. The legal system should establish vivid limits of application of such technology as facial recognition, usage of cell phones in surveillance and gathering of biometric data to assure that they are not used to carry out surveillance of large numbers of people in peaceful formations. The surveillance machines should also be controlled through other legal means by enacting legislations because any limitation to the right to assemble is not illegal and it has a purpose (Zuboff, 2019).

### 2. Supervision and Control Systems.

They should possess self-managing agencies that will oversee and control the state and corporate surveillance. Government institutions, companies, and online sites should be permitted to cheque such institutions so that they are not in violation of the legal and ethical provisions. The control mechanisms will be open and publically visible and be able to probe and penalise illegal surveillance activities. Additionally, such organisations shall be empowered to have the offenders of surveillance tools subjected to court and have them judged (Gill et al., 2019).

### 3. Publicity and Surveillance Policies Openness.

One of the elements of building trust in the surveillance systems is transparency. Involvement of the citizens in the policy making process is very crucial to make sure that the citizens are heard in designing and implementation of the surveillance technologies. The governments should also be open when it comes to their use of such surveillance tools, which kind of information they are taking and what they can do to ensure that the privacy is not violated. Regular consultations of the citizens, discussions, and the role of civil society in the processes of the surveillance can be used to ensure that the surveillance policies do not conflict with the human rights (Feldstein, 2021).

### 4. Digital literacy and Privacy-Enhancing Technology.

Privacy-enhancing technology (PET) should be encouraged in an effort to ensure that privacy of people is upheld in the highly connected world. The governments and organisations should promote creation and adoption of the tools that reduce the number of personal data collection (end-to-end encryption, anonymization, and decentralised data storage). At the same time, it is also planned to make the digital literacy programmes available to provide the citizens with the knowledge they are expected to possess to maintain their privacy, learn about the dangers of digital surveillance. Such programmes are also expected to emphasise on how people can maximise their rights by using digital resources, and how to be aware of their surveillance procedures and neutralise them.

### 5. Digital Governance: Rights International Cooperation.

Digital technologies are international, thus, there is a need to work on the global level and develop a universal approach to digital surveillance and privacy protection. The states must collaborate and come up

with international regimes of rights-based digital governance, to make sure that the surveillance practises are conducted in accordance with international provisions of human rights. It is also important that the multilateral organisations, including the United Nations and the European Union, can play a decisive role in cooperation, the formation of norms, and the provision of the absence of partial suppression of the freedom of politics, democracy, and privacy by surveillance technologies (UN Human Rights Committee, 2020).

## VIII. Conclusion

### Summary of Findings

The paper has described the nexus of digital surveillance and right to assemble (peacefully) and with references to the legal, ethical and socio-political issues. Other lessons that we have learned is the fact that although most people would argue that the surveillance technologies are being employed to ensure security and order among the citizens, their excessive application may end up on their feet by infringing the basic liberty in a disproportionate manner. The Hong Kong, the United States, India and the European Union case studies state that the people over-surveil the protests not only to violate the right to assemble, but can also be added to the chilling effect because one can be afraid of joining the protest and suffocating it. Great protection is provided with legal regulations such as international standards (ICCPR and the ECHR) and regional jurisprudence and national constitutions, yet almost always they are submitted to trial because of the rising number of surveillance technologies.

Amendment of the Significance of Peaceful Assembly in Democracy.

An active democratic society means freedom of an assembly that is peaceful. It provides people liberty in speaking out, to agitate, and to hold governments responsible. It is a right of international law, a pillar of democratic participation and its safeguard is critical to the survival of the discourse and the citizen participation. The surveillance practises must be ethically thought as it may eliminate not just the privacy but also the value of the freedom of democracy.

Equilibrium in Demand of Digital Surveillance against Human Rights.

Though the digital surveillance may have the effect of maintaining national security and safety of the people, this must be moderate with the rights of the human beings, and in this case, the right to privacy, freedom of speech and right to assemble peacefully. The most significant of this is legislative reforms, control and increase of transparency, where in such a case surveillance is not a violation of democratic principles. The necessity to hold efficient privacy laws and have clear principles as to which degree surveillance technologies should be developed is pathetic all the more as digital technologies are growing more refined and proliferated.

Recommendations on Future Research.

Further studies are needed in order to know whether the current legislative systems can be useful not only to protect the rights of the assembly but also to fight the security issues. The interjurisdictional comparative analysis would give the statistics of the effect of surveillance on the marginalised population especially in the non-Western democracies. Furthermore, the new technologies will be required to study the next stage of the digital repression like the AI-controlled surveillance and predictive policing. Lastly, more activities

will be required as regards international cooperation in the development of rights based digital governance as a way of ensuring that there is consistency in the surveillance practises in a bid to conform to the international human rights standards.

**References**

1. **ACLU.** *Free Speech and Government Surveillance.* American Civil Liberties Union, 2020.
2. **Bedoya, Alvaro.** "The Color of Surveillance." *Yale Law Journal Forum*, vol. 128, 2019, pp. 240–257.
3. **Bhat, Aditya.** "Social Media Surveillance during CAA–NRC Protests in India." *Economic and Political Weekly*, vol. 55, no. 6, 2020.
4. **Bhatia, Gautam.** *Offend, Shock, or Disturb: Free Speech under the Indian Constitution.* Oxford UP, 2017.
5. **Buolamwini, Joy, and Timnit Gebru.** "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research*, vol. 81, 2018, pp. 1–15.
6. **Buttarelli, Giovanni.** "The Critical Importance of Data Protection in a Democracy." *European Data Protection Supervisor Journal*, 2019.
7. **Council of Europe.** *European Convention on Human Rights.* Council of Europe, 1950.
8. **Donohue, Laura.** *The Cost of Counterterrorism: Power, Politics, and Liberty.* Cambridge UP, 2016.
9. **European Parliament.** *General Data Protection Regulation (GDPR).* Regulation (EU) 2016/679, 2018.
10. **Feldstein, Steven.** *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance.* Oxford UP, 2021.
11. **Gill, Lex, Jesse Redeker, and Urs Gasser.** "Digital Freedoms in a Networked World." *Berkman Klein Center Research Publication*, 2019.
12. **Guariglia, Matthew.** "DHS Surveillance of BLM Protesters." *Electronic Frontier Foundation*, 2020.
13. **Kuo, Lily.** "Hong Kong Protesters Find Ways to Evade Surveillance." *The Guardian*, 2020.
14. **Lyon, David.** *The Culture of Surveillance: Watching as a Way of Life.* Polity, 2018.
15. **Mozur, Paul.** "One Country, Two Surveillance States." *The New York Times*, 2019.