International Research Journal of Commerce and Law
Volume 13 Issue 03, March 2025 ISSN: 2349-705X Impact Factor: 8.893
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

LEGAL FRAMEWORKS GOVERNING DIGITAL SURVEILLANCE AND HUMAN RIGHTS

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

Abstract

The digital surveillance is increasingly increasing in the world with surveillance of communications and metadata collection, facial recognition, surveillance devices and social media surveillance. When such actions are considered to be serious violations of the international human rights law (IHRL), states have the propensity of justifying such actions as a need to stay safe and enforce the law. The most affected rights are privacy rights, rights to free expression, right to assemble and right to effective remedy. The main international, regional, and domestic legal provisions regarding surveillance have been discussed in this paper and a comparison made regarding how these issues have been approached by the various courts and other bodies involved in their oversight. Case law such as Carpenter v. Big Brother Watch v. United States. In the case of United Kingdom, Schrems II and Puttaswamy v. The balance between the rights and the security is exhibited in Justice K.S., Union of India. International standards used to provide further guidance include the Johannesburg Principles and the Principles of Necessary and Proportionate. The paper provides a range of problems which are common: ineffective solutions, poor transparency and ineffective protections. The paper also has an end where policy recommendations have been provided on how to come up with surveillance laws that are both rights respecting and also the ones that are security assuring.

Keywords: *surveillance, privacy, freedom of expression, peaceful assembly, proportionality, oversight, facial recognition, interception, metadata, data protection.*

1. Introduction

The rise of digital technology has completely changed the nature of the way surveillance is conducted in contemporary societies. Governments have now been using sophisticated tools that enable them to collect, store and analyse the vast amounts of personal data. These are mass interception of communications, retention of metadata, biometric identification systems and monitoring of social media activity. Although this might be motivated by the need to protect national security and maintain social order, these practices present a severe threat to some core liberties, including privacy, freedom of speech and expression, and rights to peaceful assembly (OHCHR, 2018; Lyon, 2014). The dilemma is before legislators and the judiciary to draft and

implement regulations that would bring about a balance in the issues of valid security concerns and to safeguard human rights.

The most significant question that will be addressed in the given paper is as follows: How can the laws of surveillance reconcile the demands of the state security and the rights of the people? It helps to sustain a specific amount of debates. It will start by discussing international and regional standards of human rights wherein it is established that the legal basis of restraining state surveillance. Nevertheless, the key sources in the international law are International Covenant on civil and political rights (ICCPR, 1966) and the corresponding General Commentaries, namely the General Commentaries on the right of privacy (No. 16). Second, the paper also undertakes the comparative law study of the case law and the national law. The example of the case Carpenter v. is the testimonial of one of the landmark decisions that reflects new values of the United States Supreme Court. The United States (2018) needed warrants to access information about the location of cells; the European Court of Human Rights in Big Brother Watch v. Justice K.S. Puttaswamy v. In the United Kingdom, bulk interception was protected at a very highly rated level in Justice K.S. Puttaswamy v. v. (2018); and in Justice K.S. Puttaswamy v. v. (2016) in India, bulk interception was also the case that was equally high in its protection. United Kingdom (2018), bulk interception is greatly justified; and in Justice K.S. Puttaswamy v. v. (Third, effective policy changes and legal changes recommendations will be presented in the paper. In India, the constitutional right under union of India (2017) acknowledged the right of privacy, and this has influenced the legal and policy provisions of data protection and surveillance. They have been oriented towards imagining the cheques of legality, necessity, proportionality into law; autonomous authorisation and control; and towards cultivation of transparency and provision of significant remedy.

Scope: The scope of the analysis is centred on the powers of state surveillance by interception, metadata storage, biometric surveillance, device intrusion and monitoring of social media. The role played by the private sector is also not ignored, especially when firms have no other choice but to collaborate with the state surveillance initiatives (Privacy International, 2021).

2. International Standards

The international human rights law is the general guideline for evaluating the legality of state surveillance. Article 12 of the Universal Declaration of Human Rights (UDHR, 1948) establishes that no one should be arbitrarily interfered with his/her privacy, family, home or correspondence. This was subsequently made binding in the International Covenant on Civil and Political Rights (ICCPR, 1966), specifically Articles 17, 19, 21 and 22 concerning the right to assembly and association, the right to an effective remedy, respectively. All these provisions give a normative base against which the surveillance laws and practices ought to be evaluated.

These requirements have been clarified by the UN Human Rights Committee (HRC) by its General Comments. According to the General Comment No. 16 (1988), the right to privacy may be construed in that the surveillance should be just, and the necessity and proportionality. The right of assembly that is defined in General Comment No. 37 (2020) and the freedom of expression that is defined in the General Comment No. 34 (2011) specifically state that network disruptions and digital surveillance directly affect the democratic participation. The resolutions of the UN Human Rights Council accusing the mass surveillance and the blanket internet bans without any reasonable protection have been passed as well (HRC, 2014; 2016).

Together with treaty law, there are the principles of soft law. One of the earliest credible statements making it clear that national security limitations to rights need to be strictly necessary and proportionate came in the Johannesburg Principles (1995). This was extended by the Tshwane Principles (2013), which were concerned with the equilibrium of national security and information access. The principles of communications surveillance, especially the Necessary and Proportionate Principles (2013), adopted by civil society and experts, particularly stipulate the standards of surveillance, with the emphasis on independent oversight, transparency, and effective remedies. The warnings of the chilling effect of bulk surveillance and biometric monitoring have been issued repeatedly by UN Special Rapporteurs on freedom of expression and privacy (Kaye, 2015; Cannataci, 2018). These standards are further consolidated in the OHCHR report on the right to privacy in the digital age (2018) that calls on states to revise outdated surveillance laws.

These sources develop four basic tests, including (i) Legality The laws authorising surveillance must be transparent, specific, and predictable; (ii) Legitimate Aim Surveillance must be intended only to the familiar goals such as national security or civilian safety; (iii) Necessity and Proportionality The measures to surveillance must be highly necessary, and minimum, and (iv) Safeguards and Remedies There must be independent control of surveillance, it must have transparent mechanisms, and it must have access to the redress of the law. These are the principles that are established on the international law of digital surveillance.

3. Regional Frameworks

3.1 Europe

Europe has worked out the most elaborate regional standards on surveillance. Privacy is guaranteed in the European Convention on Human Rights (ECHR), which provides the freedom of expression (Article 10), the freedom of assembly (Article 11), and the freedom of religion (Article 8). The rights are further supported by the EU Charter of Fundamental Rights, especially Articles 7 and 8, which specifically safeguard private life and personal data. European Union law goes even further and provides these protections by the General Data Protection Regulation

(GDPR, 2016) and the ePrivacy Directive (2002/58/EC). Continuing discussions of the EU Artificial Intelligence Act include the dangers of using biometric identification and algorithmic surveillance. Limits have been determined through courts: in the case of Big Brother Watch v. In United Kingdom (ECtHR, 2018), the court declared that the powers of bulk surveillance had to be heavily safeguarded, in Digital Rights Ireland (CJEU, 2014), the blanket communications data retention was found to be invalid as disproportionate, and in Schrems II (CJEU, 2020) the transfers of personal data abroad to the United States were deemed as invalid because of insufficient protection.

3.2 Inter-American System

The American Convention on Human Rights also offers privacy (Article 11) and expression rights (Article 13) to the level of ICCPR. The Inter-American Court of Human Rights has been aggressively reviewing surveillance. In Escher et al. v. Brazil (2009), it was decided that the wiretapping by the state on trade union members breached the right to privacy, right to association and right to due process. The case highlighted that the law should closely control surveillance, and the courts should be able to monitor this, and be carried out with justifiable reasons.

3.3 African System

Article 9 of the African Charter on Human and Peoples' Rights gives the right to expression, Articles 10-11 give the right to association and assembly respectively. The African Commission on Human and Peoples Rights made its Declaration of Principles on Freedom of Expression and Access to Information (2019) that explicitly prohibits indiscriminate mass surveillance and calls on reasonableness, necessity and proportionality. Other cases and statements made by high-ranking cases also criticised long-term internet blockages during elections and demonstrations because it would be disproportionate restrictions on rights as well.

3.4 Asia-Pacific

The ASEAN Human Rights Declaration (2012) has a tremendous impact on privacy and expression in the Asia-Pacific because no regional court governing it is in existence. Domestic courts hence form protections. In Puttaswamy (2017), India declared the right to privacy, in PUCL (1996), restricted electronic surveillance of the telephone and in Anuradha Bhasin (2020), restricted the internet shutdown indefinitely. The Digital Personal Data Protection Act (2023) creates more protections, although states give it wide exemptions. In the UK, bulk surveillance is governed by Investigatory Powers Act (2016). Some of the cases in the US that strengthened the privacy against intrusive searches include Katz (1967), Riley (2014) and Carpenter (2018).

4. Methodology

With the aim of analysing the consistency of digital surveillance systems with the international human rights standards, this study has been based on a comparative legal perspective. The study is organised in three levels. It starts with a review of international treaties and principles, such as the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the substantive interpretative guidelines, such as the Johannesburg Principles (1995) and Necessary and Proportionate Principles (2013). Second, it examines the regional human rights systems, with a jurisprudence of the European Court of Human Rights, the Inter-American Court of Human Rights, and the African Commission. Third, it assesses the national legislation and prominent court rulings, such as the cases of the United States, the United Kingdom, India, and Brazil. Along with the analysis of doctrine, the study uses empirical sources including UN Special Rapporteur reports, corporate transparency reports, and civil society datasets regarding internet shutdowns as a way of evaluating the legality, necessity, proportionality, and safeguards of state practice.

5. Case Studies

5.1 United States

Digital surveillance in the United States has been a central focus of judicial review based on the fourth amendment of the right against unreasonable searches. In Riley v. The Supreme Court in California (2014) ruled that a mobile phone should be warranted by the police as it contains vast information about the individual. This was further extended in Carpenter v. United States (2018), in which the Court decided that a warrant is also necessary when historic information about cell-site location is accessed. Nevertheless, in spite of these developments, massive surveillance under the Foreign Intelligence Surveillance Act (FISA), especially the 702 section has been controversial, and critics believe that it lacks control and poses threats to individual privacy (Swire & Hemmings, 2019).

5.2 Europe

The European courts have significantly been involved in setting boundaries on federal surveillance. In Big Brother Watch v. In United Kingdom (ECtHR, 2018), the European Court of Human Rights appreciated the lack of protection in the bulk interception system of the UK to be in breach of Article 8 and 10 of the ECHR. The Court of Justice of the European Union (CJEU) has continuously objected to mass collection of data, prohibiting indiscriminate metadata-retention legislation in Digital Rights Ireland (2014) and La Quadrature du Net (2020) on the basis of proportionality. The CJEU in Schrems II (2020) also struck down the EU–US Privacy Shield on the ground of insufficient protection against US surveillance.

5.3 India

Privacy as a fundamental right in Justice K.S. Puttaswamy v., the Supreme Court has developed the Indian constitutional jurisprudence considerably. Union of India (2017). Earlier, in PUCL v. The Court provided protection against telephone interception and procedural supervision in Union of India (1996). Also more recently, Anuradha Bhasin v. Union of India (2020) found that the indefinite internet shutdowns were unconstitutional and the proportionality in blocking communications was important. The Digital Personal Data Protection Act (2023) is a new data-protection law in India, yet its critics claim that its large state exemptions undermine personal privacy rights and negate its efficacy (Bhandari and Purohit, 2023).

5.4 Brazil

In Escher et al. v. Brazil (IACtHR, 2009), the Inter-American Court of Human Rights held that the monitoring of the members of a trade union by the state infringed upon the right to privacy and association provided in the American Convention. The Court indicated that surveillance must be law-based, restricted in extent and must undergo judicial review. This case continues to be a major contributor to the Inter-American system on the threat of unchecked state surveillance.

6. Discussion

As the comparative analysis shows, despite the fact that numerous states have developed legislation permitting surveillance, such frameworks are often inadequate in comparison to the international human rights standards. One of the common problems is the application of vague and over broad laws, which leave extensive discretion in the hands of the executive. Such legal provisions do not pass the test of legality because citizens do not have any reasonable expectation of how wide and far they are being surveilled by the state (HRC, General Comment No. 16, 1988). The other weakness is the absence of independent authorisation. In various jurisdictions, executive authorities or security agencies grant surveillance orders, but without having to seek judicial permission beforehand. This compromises the principle of safeguard, which demands autonomous and independent supervision. To take one example, discussions of FISA Section 702 in the United States demonstrate the fear that intelligence services can exercise immense authority without a court check (Swire and Hemmings, 2019). Likewise, at the same time, interception authority is concentrated within administrations in most African and Asian nations, instead of independent courts, which creates issues of accountability (ACHPR, 2019).

Checking and balancing systems and solutions are also poor. Civil society transparency reports indicate that people often do not have a way to take on unlawful surveillance because of secrecy laws, and without prior notice (Access Now, 2022). Where remedies exist, they are usually ineffective or slow; thus, individuals are not afforded any meaningful protection. Another problem

is the overuse of national security exceptions. States will frequently use national security a priori to seal off mass surveillance, internet blockages or demands on data localisation. Security is a valid purpose, but international standards also stipulate that restrictions must be both necessary and proportionate and be the least intrusive possible (OHCHR, 2018). Unjustified data retention, as observed in Digital Rights Ireland (2014) and La Quadrature du Net (2020) cases by the CJEU, depicts the threats of the disproportional actions.

7. Recommendations

According to the results of this paper, it is necessary to implement a number of policies and legal changes that would allow harmonising the surveillance framework with the international human rights requirements.

1. Clear Laws: The surveillance should be clearly sanctioned by clear and foreseeable legislation. Laws that are vague and leave wide powers to executive agencies are prone to abuse and do not pass the test of legality under international law (HRC, General Comment No. 16, 1988). The extent, time, and the allowed use of the surveillance should be spelt out in laws.

2. Necessity and Proportionality: Only under strict necessity and in proportion to a legitimate purpose, like a national security purpose or a serious crime prevention purpose, should surveillance be utilised. The Johannesburg Principles (1995) and the Necessary and Proportionate Principles (2013) point out that bulk or indiscriminate collection is seldom justified, and targeted approaches should be given a priority.

3**. Independent Oversight:** The granting of surveillance should be by the hands of judges or independent control institutions and not political power. This has been highlighted by the European Court of Human Rights on numerous occasions in cases that involve independent ex ante review as it was the case with Big Brother Watch v. UK (2018). Depending on judicial authorisation should also have regular audits and other reporting mechanisms.

4. Transparency: The governments should publish regular transparency reports concerning the quantity and character of surveillance orders, internet interruptions, and data orders. It is consistent with the decisions of the UN Human Rights Council (2014, 2016) that require the transparency of surveillance practises. It should also be disclosed that the aggregate government requests are made by the private companies so that they could be scrutinised independently (Access Now, 2022).

5. Effective Remedies: People should be given the right to oppose unlawful surveillance. The courts are supposed to give prompt and available redress, such as recompense or the removal of illegally acquired data. Effective remedies are assured through the ICCPR Article 2(3), which is not well exercised in most jurisdictions.

6. International Cooperation: Due to the cross-border flows of data, global collaboration is a responsibility. Data sharing frameworks should be made to comply with international standards of privacy, as highlighted in Schrems II (CJEU, 2020). The safeguards provided by the GDPR and other robust data protection regulations should be provided in bilateral and multilateral agreements.

8. Conclusion

One of the hottest issues of contemporary democracies is digital surveillance. Although states claim that these powers are important in fighting terrorism and security in the country, unrestrained surveillance violates basic rights. An excellent framework is given by international law: legality, necessity, proportionality and protection. Courts in India and the United States have also helped to expand the amount of privacy protections, although there are still serious gaps in the enforcement of these systems, particularly in Europe and America. Accountability is compromised by vague legislation and a lack of adequate supervision and national security exemptions. States need to restructure their surveillance systems to support rights-based standards as a way of preserving democratic governance. This is because the future of surveillance governance lies in the development of systems that are already transparent, accountable, and respectful of human dignity (OHCHR, 2018). It is only at this point that societies can meet a compromise between legitimate security interests and guaranteeing the protection of individual freedoms.

References

1. Access Now. (2022). *KeepItOn: Internet shutdowns report* (pp. 10–25). Access Now. https://www.accessnow.org/keepiton
2. ACHPR. (2019). *Declaration of principles on freedom of expression and access to information in Africa*. African Commission on Human and Peoples' Rights.
3. Article 19. (1995). *Johannesburg principles on national security, freedom of expression and access to information*. Article 19.
4. ASEAN. (2012). *ASEAN human rights declaration*. ASEAN Intergovernmental Commission on Human Rights.
5. Bhandari, V., & Purohit, S. (2023). *The DPDP Act and state surveillance* (pp. 4–9). Internet Freedom Foundation. https://internetfreedom.in
6. Cannataci, J. (2018). *Report of the Special Rapporteur on the right to privacy*. UN Doc. A/HRC/37/62 (pp. 5–16). United Nations.
7. Council of Europe. (1950). *European convention on human rights*. Rome, 4.XI.1950.
8. European Union. (2000). *Charter of fundamental rights of the European Union*. Official Journal of the European Communities, C364/1.

9. European Union. (2002). *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive)*. Official Journal of the European Communities, L201, 37–47.
10. European Union. (2016). *General data protection regulation (GDPR)*, Regulation (EU) 2016/679. Official Journal of the European Union, L119, 1–88.
11. Kaye, D. (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. UN Doc. A/HRC/29/32 (pp. 3–12). United Nations.
12. Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, 1(2), 1–13. https://doi.org/10.1177/2053951714541861
13. Necessary and Proportionate Principles. (2013). *International principles on the application of human rights to communications surveillance*. https://necessaryandproportionate.org
14. OHCHR. (2018). *The right to privacy in the digital age*. Report of the Office of the High Commissioner for Human Rights, UN Doc. A/HRC/39/29 (pp. 6–18). United Nations.
15. Open Society Justice Initiative. (2013). *The Tshwane principles on national security and the right to information*. OSJI.
16. Privacy International. (2021). *State of privacy: Global report* (pp. 22–35). Privacy International.
17. Swire, P., & Hemmings, K. (2019). *Reforming Section 702 of FISA* (pp. 15–20). Georgia Tech Research Paper.
18. United Nations. (1948). *Universal declaration of human rights*. United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-right
19. United Nations. (1966). *International covenant on civil and political rights*. United Nations Treaty Series, 999 U.N.T.S. 171.
20. UN Human Rights Committee. (1988). *General Comment No. 16: The right to privacy (Article 17)*. UN Doc. HRI/GEN/1/Rev.1.
21. UN Human Rights Committee. (2011). *General Comment No. 34: Freedoms of opinion and expression (Article 19)*. UN Doc. CCPR/C/GC/34.
22. UN Human Rights Committee. (2020). *General Comment No. 37: Right of peaceful assembly (Article 21)*. UN Doc. CCPR/C/GC/37.
23. UN Human Rights Council. (2014). *The right to privacy in the digital age*. UN Doc. A/RES/68/167.
24. UN Human Rights Council. (2016). *The right to privacy in the digital age*. UN Doc. A/HRC/RES/34/7.

Case Law

1. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
2. *Big Brother Watch and Others v. the United Kingdom*, App Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R. (2018).

3. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
4. *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, Case C-311/18, CJEU (2020).
5. *Digital Rights Ireland Ltd v. Minister for Communications*, Joined Cases C-293/12 and C-594/12, CJEU (2014).
6. *Escher et al. v. Brazil*, Inter-Am. Ct. H.R. (Ser. C) No. 200 (2009).
7. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
8. *Katz v. United States*, 389 U.S. 347 (1967).
9. *La Quadrature du Net v. France*, Case C-511/18, CJEU (2020).
10. *People's Union for Civil Liberties (PUCL) v. Union of India*, AIR 1997 SC 568 (India).
11. *Riley v. California*, 573 U.S. 373 (2014).