International Journal of Trade and Commerce-IIARTC
July-December 2024, Volume 13, No. 2, pp. 384-392
ISSN-2277-5811 (Print), 2278-9065 (Online)

COSMOS (Germany) JIF: 5.135; ISRA JIF: 7.249; ISI JIF: 3.721

CCTV Cameras Surveillance System vis-à-vis Right to Privacy

Mohammed Danish Khan[a]*, Uzma Ansari[b]
[a]Faculty of Law, Meerut College, Meerut, U.P., India
[b]Faculty of Law, Aligarh Muslim University, Aligarh, U.P. ,India
E-mail: dkdanish.khan001@gmail.com[a], ansariuzma843@gmail.com[b]

Abstract

In the context of today's high-tech video surveillance which includes smart cameras, video surveillance systems, biometrics, and facial recognition, the protection of an individual's privacy is increasingly being raised. High-tech CCTV surveillance systems which gather information and data on individuals, have become commonplace because of their security benefits. However, because the public has little control over personal data, such proactive surveillance put the privacy of individuals at risk. With regard to the principle of proportionality and justifiable interests, biometric remote identification can be carried out with specific protections. Currently, the CCTV surveillance system is a very contentious and expanding surveillance technology. While it is pertinent to security, on the other hand it is widely criticized by many people for its misuse. The "Real Time" biometric identification of people in public areas for law enforcement reasons significantly violates people's liberties and private rights. Furthermore, video monitoring has the potential to record sensitive information. Thus, the rules outlined in privacy legislation must be followed by such surveillance systems. The personal life of people may be impacted by the unlawful use of personal data. Any processing of personal data must respect basic rights, such as the right to privacy, family rights, and the protection of personal data, as per EU Directive no. 2019/790 on Copyright and Related Rights.

This paper comprehensively discusses the multifaceted impacts on individuals' privacy as well as new challenges regarding privacy preservation that are raised due to CCTV footage surveillance. Through a comprehensive analysis of existing literature, this paper offers insight into the benefits and drawbacks of CCTV surveillance systems and highlights the need for balanced approaches between public safety and individual privacy.

Key Words: *CCTV Camera, Surveillance System, Privacy, Security, Freedom, Regulations, Public Safety.*

PAPER/ARTICLE INFO
RECEIVED ON: 22/11/2024
ACCEPTED ON: 29/12/2024

Reference to this paper should be made as follows:

Khan, Mohammed Danish & Ansari, Uzma (2024), "CCTV Cameras Surveillance System vis-à-vis Right to Privacy", *Int. J. of Trade and Commerce-IIARTC*, Vol. 13, No. 2, pp. 384-392.

**Corresponding Author*
DOI: 10.46333/ijtc/13/2/13

1. INTRODUCTION

The history of video surveillance begins in the middle of 20th century, when **Walter Bruch** created **Closed-Circuit Television (CCTV)** technology, which was first used to capture live footage in Germany. This rudimentary form of CCTV was employed to watch V-2 missiles during the war. The commercial of CCTV systems did not occur until 1949, a span of seven years. Furthermore, since technology advanced so quickly in recent years, its broad use started to take root gradually. In the present digital era, the right to privacy is a right which is protected as a fundamental right in almost every country in this world. Generally speaking, this right refers to a person's freedom from all interference and intrusion. Various scholars have tried to define the word 'Privacy' but this word has been used as a legal concept in the last century. Protecting privacy protection is a major problem in today's technologically advanced culture. The meaning of privacy varies according to the legal, social, political, cultural, and technological contexts. Privacy is a personal right that regulates how much private information is used and how much personal information being disseminated to the public.[1] Some people prioritize privacy on the other hand some may prioritize security and monitoring. When personal data is gathered and shared without permission, privacy issues occur. It is possible for personal information to be collected and shared without an individual's knowledge. The biometric information of users is vulnerable to misuse and unauthorized access, and data collected for certain objectives may be used illegally. There are security issues since it may be copied or erased and used for other reasons.

2. THE CONCEPT OF PRIVACY

In the International Human Rights Laws, the concept of privacy is contentious. Divergent views exist across nations about the constitutional right to privacy. Law enforcement officials and legislators disagree on the definition of "privacy" and how it differs from other fundamental rights. Every person in the world has the right to privacy. Every human being has the constitutional right to govern their own private lives, and no one or any organization is permitted to unlawfully access another person's private place, belongings, or information.[2] Each person has authority over their personal data in several spheres of their lives. As Serohin Vitalii put it: "Information privacy is a certain imprint of a person's private life in the form of certain information (data) about the relevant facts, phenomena, and events that relate to a person's life and this information is a priori confidential."[3]

3. GLOBAL PERSPECTIVE ON THE RIGHT TO PRIVACY

Numerous international treaties and instruments have acknowledged the right to privacy as a basic human right. Article 12 of the **Universal Declaration of Human Rights (UDHR) 1948** provides "No one shall be subjected to arbitrary interference with his privacy, family, home or

[1] Sekione, Oscar, Oscar Enrique, Jong Hyuk, Pradip Kumar, "CCTV Footage De-Identification for Privacy Protection A Comprehensive Survey" 25 *Journal of Internet and Technology* 379-386 (2024).

[2] Ali Alibeigi, Abu Bakar Munir, Md Ershadul Karim, "Right to Privacy; A complicated Concept to Review" *Library Philosophy and Practice (e-journal).* 2841(2019).

[3] Vitalii, Serohin, "Information Privacy: A Conceptual Approach" *Constitutional and Legal Academic Studies* 52-60 (2020).

correspondence, nor to attack upon his honor and reputation"[4]. **S**imilarly, Article 17 of **the International Covenant on Civil and Political Rights (ICCPR) 1966** guaranteed the protection against arbitrary and illegal interference with privacy.[5] The protection of privacy has faced new challenges in the digital age. The Resolution 68/167 on "The Right to Privacy in the Digital Age" was approved by the United Nations Human Rights Council adopted in 2013, emphasizing the rights that individuals have offline, and must be protected online.[6]

4. IMPACT OF TECHNOLOGY ON PRIVACY RIGHTS

Human existence is greatly impacted by technology. The quick development of home security devices, particularly Closed-Circuit Television Cameras, is another effect of growing technology.[7] CCTV footage includes multimedia such as images, audio, and video. Computer vision is a useful technology to identify and comprehend visual data to extract information that raises privacy breaches. CCTV cameras are a tool used by homeowners for both indoor and outdoor monitoring. For instance, CCTV cameras are typically installed by homeowners to keep an eye on criminal activities in residential areas.[8] One's right to privacy is violated by the usage of CCTV cameras and other surveillance equipments. Therefore, there should be a definite reason to use these devices. Moreover, the use of such surveillance devices can result in privacy breaches. Technological advancements have tremendously enhanced search, seizure, and surveillance systems and improved the quality of video surveillance but this leads to privacy breaches. The excessive development of digital technologies makes it easy to collect personal data and their storage. The capabilities and facilities of video surveillance systems, sometimes referred to as closed-circuit television (CCTV), have been improved by modern technology, which have also improved the use of surveillance. Additionally, wireless networks, multispectral image sensors, and intelligent multi- camera networks have aided surveillance systems in recent years. However, these advancements raised various privacy concerns because they can store and analyze various personal data. Therefore, it is pertinent that before installing such surveillance devices, everyone must pay heed to the privacy rights of others.

Failure the protection personal data will lead to destruction, loss, and unauthorized dissemination of personal data which will raise privacy concerns. The application of CCTV recording and surveillance is justified as it helps to maintain security and prevent crimes as it captures the movement of the object as well as the individual in the form of images and videos. Many developed countries have installed millions of surveillance systems to prevent crimes as well as to predict any distress or peril in public. However, these surveillance systems raise a significant concern regarding privacy protection which is an important right of every human

---

[4] United Nations Universal Declaration of Human Rights, 1948, Article 12.

[5] International Convention on Civil and Political Rights, 1966, Article 17.

[6] Niyigena Miguel, *Legal Analysis of the Effects of Digital Surveillance on Individuals' Right to Privacy under Rwandan Legal Framework* (2024) (Unpublished LL.B. Dissertation, Kigali Independent University ULK).

[7] Muhammad Faisal Hilmi Gunawan, "Private CCTV Liabilities under Biometric Data Protection Rules", 2, *Jurnal Inovasi Global* (2024).

[8] J Dahmen, B.L.Thomas, L. Brian, D. Cook, J., & Wang, Xiaobo, "Activity learning as a foundation for security monitoring in smart homes", 17 *Sensor* (2017).

being. There are many technologies such as Google Street View, Yandex Maps, Bosch Security System, Hikvision, Zicom Electronic Security Systems, etc. which provide panoramic images but these services raise serious privacy concerns all over the world. These technological advancements take the images of roads, streets, communities, and even private places without taking consent of the people. Thus, the rights of an individual may be infringed. By eliminating and altering personal identifiers in CCTV footage and other multimedia information, further precautions should be made to preserve privacy in this respect.

5. REASONS WHY CCTV INSTALLATIONS ARE REQUIRED

- **Prevention of crime and violence:** CCTV cameras assist in deterring criminal activities such as theft, vandalism, bullying, and assault. The presence of cameras can prevent potential offenders from engaging in illegal or harmful behavior. Studies show that where CCTV cameras have been installed, the criminal activities have been significantly decreased. A study shows that "The number of robbery and theft reduced by 47.4 % in the area where CCTV cameras were installed".[9]
- **Incident response:** In the event of an incident, CCTV footage can provide critical evidence to identify and apprehend offenders, ensuring a swift response by security personnel or law enforcement. The majority of participants said that they felt safer with the presence of CCTV Camera". [10]
- **Deterrence of misconduct:** The installation of CCTV cameras can discourage people from engaging in misconduct or other inappropriate behavior.
- **Evidence collection:** CCTV footage provides valuable evidence in investigations of incidents ranging from minor infractions to serious crimes. This assists in making informed decisions and ensuring justice.
- **Verification of events:** Surveillance footage can verify accounts of events provided by witnesses, providing a clear and unbiased perspective on incidents.
- **Real-time monitoring:** Security personnel can monitor live feeds to detect and respond to emergencies such as fires, medical incidents, or intrusions swiftly.
- **Coordination with authorities:** In emergencies, CCTV footage can be shared with law enforcement or emergency responders to provide accurate information about the situation.
- **Risk management:** CCTV installation helps in managing risks by documenting incidents and protecting against liability claims related to safety and security breaches.
- **Global security concerns:** in a global context marked by heightened security concerns, CCTV surveillance systems address potential threats such as terrorism and mass violence.

[9] H.H. Park, G. Oh, and S. Y. Paek, "Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea", 40 *International Journal of Law, Crime and Justice* 179-191(2012).

[10] B. R. Ardabili et al., "Exploring Public's Perception of Safety and Video Surveillance Technology: A survey approach", 78 *Technology in Society* (2023).

6. PROBABILITY OF PERSONAL INFORMATION BEING MISUSED AND ABUSED VIA CCTV SURVEILLANCE

The probability for misuse or abuse of personal information through CCTV surveillance systems is a significant concern due to the following factors:

- **Unauthorized access by the third party:** Data collected through CCTV may be shared with third-party contractors and companies, creating a potential risk of misuse. These third parties may not always have the same privacy standards and security measures as the original operators, increasing the risk of mishandling or unauthorized distribution of data. Without strict access controls, unauthorized individuals might gain access to surveillance footage, leading to potential breaches of privacy and misuse of information.
- **Privacy Invasion:** CCTV cameras capture highly personal and sensitive information about individuals such as their movements, interactions, and behavior in public and private spaces. This can lead to a loss of personal privacy.
- **Data Breaches:** Surveillance data, if not properly secured, can be vulnerable to hacking and unauthorized access. If this data is breached, it can expose sensitive information. This data can be used for identity theft, stalking, or other malicious activities.
- **Surveillance Overreach:** Governments and organizations can use CCTV systems to engage in mass surveillance, collecting data on individuals without their consent. This could lead to discriminatory practices, such as targeting specific demographics or individuals for monitoring based on race, religion, or political views.
- **Lack of Accountability:** In some cases, individuals or entities responsible for managing surveillance systems may not be held accountable for how they handle personal data. Without clear oversight, data may be misused, for example, by storing excessive footage or using it for purposes outside the original intent such as profiling or monitoring political activities.
- **Inappropriate Monitoring:** There is a risk that CCTV systems could be used to monitor individuals for purposes beyond security, such as tracking the movements of specific people or groups without a legitimate reason. This can lead to discrimination, harassment, or other forms of abuse.
- **Data Manipulation and Fabrication:** The integrity of CCTV footage must be maintained to ensure it is reliable for investigation and evidence. Any Manipulation or fabrication of footage can result in wrongful accusations or the failure to hold accountable those responsible for misconduct.
- **Chilling Effect:** The constant monitoring of public spaces can lead to "Chilling Effects" where people feel they are always being watched. This can deter freedom of expression and movement as people may avoid participating in certain activities and expressing opinions due to fear of surveillance.

Data protection laws require that the people in charge of the equipment be held accountable for data breaches when a person's private information is illegally obtained through a domestic CCTV surveillance system. The UK PDPA states that, a controller who violates data protection laws may face consequences. In addition, there are many provisions relating to privacy rights exercised by

an individual under the UK Personal Data Protection Act, of 2018. Apart from this if the breached data are sensitive then the data subject is entitled to get notified without any unnecessary delay.

7. LEGAL AND ETHICAL CONSIDERATIONS

Legal considerations are paramount when installing CCTV systems in public places such as streets, markets, roads, institutions, etc. These considerations include adherence to data protection and privacy laws, which differ from one country to another but generally work to safeguard an individual's right to privacy and the security of their personal information. On the other hand, ethical guidelines focus on respecting the rights and dignity of individuals affected by CCTV Surveillance. These guidelines emphasize the need for consent, transparency, and accountability in surveillance practices. Before installing a CCTV system everyone must consider:

- **Understand Privacy Laws:** Familiarize themselves with national and regional laws that govern surveillance and personal data protection, such as the General Data Protection Regulations (GDPR) in Europe and the Digital Personal Data Protection Act in India.[11]
- **Implement Data Protection Measures:** Ensure data collected through CCTV systems is stored securely and accessed only by authorized personnel and used only for the intended purpose. This includes encrypting data, setting strict access controls, and establishing clear data retention policies.
- **Conduct Privacy Impact Assessments (PIAs):** Regularly assess the impact of CCTV systems on privacy and mitigate potential risks through appropriate measures. PIAs help in identifying and addressing any privacy concerns before implementing surveillance.
- **Obtain Consent:** The explicit consent of the data subjects is required before monitoring. While it may not be feasible to get consent from data subjects about the presence of a CCTV system.
- **Ensure Transparency:** Inform stakeholders about the presence of CCTV cameras, their location, and the specific purposes for which surveillance is conducted. Putting signs about CCTV camera installation might help in maintaining transparency.
- **Maintain Accountability:** Establish mechanisms to hold those responsible for CCTV operations accountable. This includes setting up clear protocols for monitoring, accessing, and handling surveillance data, as well as regular audits and reviews of CCTV practices.[12]

8. REGULATORY FRAMEWORKS AND GUIDELINES

Numerous protections for the right to privacy pertaining to people, groups, and organizations are included in privacy regulations. These regulations address the privacy legislation regarding the acquisition, retention, and use of personal information by the government. Privacy is protected by the data privacy laws. These laws provide guidelines to companies and organizations on how to

[11] Available at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[12] Samirsinh P Parmar, Swati H Chauhan, "Legal and Ethical Guidelines in CCTV Surveillance: Addressing Key Issues in Educational Institutions", 6 *International Journal of Human Rights and Constitutional Studies* 14-28, (2024).

collect and store data along with how to notify data subjects. Additionally, they restrict the amount of control that a data subject has over the data once it has been conveyed. Many countries have taken steps to enact laws to secure personal data and safeguard individual privacy. In 2018, significant progress was made in the areas of data privacy and privacy safeguards. European Union introduced the data protection regulations in 2018 which is called **General Data Protection Regulations (GDPR). C**omprehensive guidelines for the entities' data collecting and data processing are provided by this regulation. The purpose of these regulations was to uphold the confidentiality of the people's personal information. After the European Union, California introduced the **California Consumer Privacy Act (CCPA) in June 2018.** Eventually**,** the **Singapore Personal Data Protection Act (SPDP)** came into effect. In July 2018, India also introduced a draft bill to protect the personal data which was named as **Indian Personal Data Protection Bill (PDPB). Now PDPB in 2023 has been enacted as an act named Digital Personal Data Protection Act (DPDPA).** However, many countries such as Malaysia, Thailand, Vietnam, etc. also adopted data protection laws. These privacy protection laws provided that if any person, government, organization, etc. collected the personal data of individuals they were bound by these laws. [13] .

The main principles related to privacy regulations under GDPR, PDPA, etc. can be summarized as follows:

- **Right to Know/ Right to Consent**: One of the most important principles provided by Sections 13 to 17 of PDPA and Articles 19 and 24 of GDPR is the right to be informed or the right to get consent. Every individual must have the right to provide their express consent before any personal data is collected. Section 18 places restrictions on the uses, disclosures, and collection of personal data.
- **Right of Access:** people have the right to ask for access to and correction of their personal data under Sections 21, 22, and 22A of PDPA. The data subject shall be provided with access authorization and a copy of their processed personal data upon request. Security measures are provided under Section 24 of PDPA to protect personal information and reduce the danger of unauthorized access.
- **Right to Object:** Article 21 of GDPR stipulates that the data subject has the right to withdraw the consent. The processing of personal data may be objected to at any time by the data subject. This right guarantees the accuracy and responsibility of the information gathered. The accuracy and completeness of the data are guaranteed under Section 23. If the information is inaccurate then the data subject has the right to object and rectify the information stored.
- **Right to Restrict Processing:** Article 18 of GDPR provides that individuals have the right to restrict their data in any situation. Additionally, the controller may be asked to halt processing by the data subject.

[13] Kajal Kansal, Yongkang Wong, Mohan S. Kankanhalli, "Implication of privacy regulations on video surveillance systems", *ACM Transaction on Multimedia Computing, Communications and Applications* DOI 10.1145/3706108 (2024).

- **Right to Data Portability:** According to Article 20 of the GDPR, the data subjects are entitled to utilize their data for various purposes across various services. Article 20 also ensures that the data subjects can move, copy, and transfer their data but section 26 of PDPA prohibits the transfer of personal data.
- **Right to be Forgotten:** Article 17 of GDPR ensures that data subjects have the right to be forgotten. They have the option to ask the controller to remove their information. Companies are required by law to do this and their systems need to be able to remove data subjects' personal information upon request. However, the right to be forgottenis not supported by the PDPA.

9. CONCLUSION

In this paper general overview regarding public safety as well as the right to privacy has been presented. This paper has additionally mentioned the importance and necessity of CCTV surveillance systems installation to prevent criminal activities as well as legal and ethical considerations. While installing CCTV cameras it is very important to consider an individual's privacy right. In the light of today's sophisticated video surveillance, which uses smart cameras, video surveillance systems, biometrics, and face recognition, the protection of the privacy of an individual is increasingly called into question. The preservation of private rights is a top priority, even if there are several legislative frameworks such as UDHR, GDPR, ICCPR, DPDPA, etc. that offer guidance for the protection of privacy rights of individuals. Therefore, it is crucial to access the necessity and efficacy of monitoring techniques in the context of individual privacy. A sophisticated strategy is needed to strike a balance between the governments' justifiable public safety concerns and the basic right to privacy. Establishing a more equal connection between technology and privacy requires openness in data collecting procedures, robust consent procedures, and the ability of individuals to manage their data. While preventing crime is an important social goal, the right to privacy in public is comparatively limited. It should be illegal to rely on privacy as a cover for illegal activity. Ironically, the necessity for monitoring is what drives the demand for privacy. The state must interfere in the lives of its inhabitants in a variety of circumstances, such as to deter crime, but this interference must be grounded on and constrained by fundamental laws. Thus, there should be a balance between individual privacy and public safety.

REFERENCES

[1]. Sekione, Oscar, Oscar Enrique, Jong Hyuk, Pradip Kumar, "CCTV Footage De-Identification for Privacy Protection A Comprehensive Survey" 25 Journal of Internet and Technology, pp. 379-386 (2024).
[2]. Ali Alibeigi, Abu Bakar Munir, Md Ershadul Karim, "Right to Privacy; A complicated Concept to Review" Library Philosophy and Practice (e-journal). 2841(2019).
[3]. Vitalii, Serohin, "Information Privacy: A Conceptual Approach" Constitutional and Legal Academic Studies, pp. 52-60 (2020).
[4]. United Nations Universal Declaration of Human Rights, 1948, Article 12.
[5]. International Convention on Civil and Political Rights, 1966, Article 17.

[6]. Niyigena Miguel, Legal Analysis of the Effects of Digital Surveillance on Individuals' Right to Privacy under Rwandan Legal Framework (2024) (Unpublished LL.B. Dissertation, Kigali Independent University ULK).
[7]. Muhammad Faisal Hilmi Gunawan, "Private CCTV Liabilities under Biometric Data Protection Rules", 2, Jurnal Inovasi Global (2024).
[8]. J Dahmen, B.L.Thomas, L. Brian, D. Cook, J., & Wang, Xiaobo, "Activity learning as a foundation for security monitoring in smart homes", 17 Sensor (2017).
[9]. H.H. Park, G. Oh, and S. Y. Paek, "Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea", 40 International Journal of Law, Crime and Justice, pp. 179-191(2012).
[10]. B. R. Ardabili et al., "Exploring Public's Perception of Safety and Video Surveillance Technology: A survey approach", p. 78 Technology in Society (2023).
[11]. Available at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[12]. Samirsinh P Parmar, Swati H Chauhan, "Legal and Ethical Guidelines in CCTV Surveillance: Addressing Key Issues in Educational Institutions", 6 International Journal of Human Rights and Constitutional Studies, pp. 14-28, (2024).
[13]. Kajal Kansal, Yongkang Wong, Mohan S. Kankanhalli, "Implication of privacy regulations on video surveillance systems", ACM Transaction on Multimedia Computing, Communications and Applications DOI 10.1145/3706108 (2024).
[14]. Arora, Ritu (2016). The Plight of Female Domestic Workers in Urban Amritsar. International Journal of Trade & Commerce-IIARTC. 5(1), pp. 121-135.