

Digital Surveillance and the Right to Privacy: An International Law Perspective

المراقبة الرقمية والحق في الخصوصية من منظور القانون الدولي

TRIKI Cherifa*

Faculty of Law – University of Algiers 1

c.teriki@univ-alger.dz

Date of Submission 14-10-2025 Date of Final Acceptance 23-08-2026 Date of Publication September 2026

Abstract:

The nature and extent of monitoring have been drastically altered by the rapid development of digital technologies, raising serious concerns about the protection of the right to privacy. Within the context of international law, this paper examines the theoretical foundations of digital surveillance, traces the evolution of the right to privacy, and evaluates key legal frameworks that safeguard it. The study assesses the effectiveness of these frameworks in addressing modern surveillance techniques and considers the impact of surveillance by public and private actors. It argues that, although privacy is recognized as a fundamental right, existing legal systems remain structurally inadequate to regulate contemporary digital surveillance. It concludes by emphasizing the need for a more nuanced, human rights-based approach that strengthens accountability and promotes international cooperation.

Keywords: Digital Surveillance; Data Protection; International Law; Human Rights.

الملخص:

لقد أدى التطور السريع للتكنولوجيا الرقمية لتغير طبيعة ومدى المراقبة بالشكل الذي أثار تساؤلات جدية حول مدى حماية الحق في الخصوصية. تهدف هذه الدراسة للبحث في الأسس النظرية للمراقبة الرقمية، تتبع مسار تطور الحق في الخصوصية، وتبيان أهم الأطر القانونية الدولية الحامية للحق في الخصوصية والنظر في مدى فعاليتها في مواجهة تقنيات المراقبة الحديثة. تخلص الدراسة بالتأكيد على أنه بالرغم من الاعتراف الدولي بالحق في الخصوصية كأحد حقوق الإنسان الأساسية، إلا أن الأطر القانونية الحالية تظل غير قادرة على ضبط أنماط المراقبة الرقمية المعاصرة، مما يؤكد ضرورة اعتماد استراتيجية قانونية شاملة، مؤسسة على حقوق الإنسان، تعزز آليات المساءلة وتشجع التعاون الدولي في سبيل تكريس حماية فعالة للحق في الخصوصية في العصر الرقمي.

الكلمات المفتاحية: المراقبة الرقمية، حماية البيانات، القانون الدولي، حقوق الإنسان.

* Corresponding Author: TRIKI Cherifa

Introduction:

The nature, breadth, and tactics of surveillance have undergone a profound transformation in recent decades due to the rapid expansion of digital technologies. Digital surveillance functions through ongoing, extensive, and frequently undetectable processes of data gathering, analysis, and prediction, in contrast to conventional types of monitoring, which were usually restricted in scope and focused in application. Both state and non-state actors may now watch people in previously unheard-of ways thanks to the integration of artificial intelligence, big data analytics, biometric identification technologies, and international communication infrastructures.

In addition to improving the effectiveness of security and governance systems, this change has brought up serious ethical and legal questions about the defense of fundamental rights, especially the right to privacy. In the digital world, systematic data gathering, behavioral profiling, and algorithmic decision-making processes that function outside of an individual's awareness or control pose a greater threat to privacy than direct invasions or disclosures.

Simultaneously, the transnational movement of data and the globalization of digital infrastructures have made the legal environment even more complex. While legal safeguards are still mostly territorial and dispersed, surveillance techniques are no longer limited to national borders. This discrepancy raises significant regulatory issues that will be discussed later in relation to international data governance and cross-border monitoring.

In this regard, one of the most important topics in current legal discourse is the connection between digital surveillance and the right to privacy. It brings up important issues regarding the suitability of current international legal instruments, the way privacy is developing as a legal notion, and the ability of legal systems to adapt to quickly changing technological realities.

In light of systemic and technologically driven monitoring activities, this paper offers a critical reevaluation of international privacy regimes, adding to the body of literature.

1.1. Problem Statement:

Even while the right to privacy is widely acknowledged as a fundamental human right in international and regional legal instruments, the complexity brought about by contemporary digital monitoring technology seems to be beyond the scope of current legal frameworks. The fundamental issue is the structural mismatch between the relatively static, dispersed, and frequently reactive nature of legal control and the developing nature of surveillance, which is defined by its international breadth, technological sophistication, and predictive capacities. It is challenging to deal with modern types of algorithmic monitoring, biometric identification, and cross-border data processing because existing legal frameworks were mostly created prior to the advent of widespread digital surveillance.

As a result, a gap emerges between the formal recognition of privacy rights and their effective protection in practice, particularly in the context of large-scale, data-driven, and algorithmically mediated surveillance systems. Considering the aforementioned, the main question of the study is:

To what extent are existing international legal frameworks capable of effectively protecting the right to privacy in the face of contemporary digital surveillance practices?

To address this main question, the study seeks to answer the following sub-questions:

- How has the legal concept of privacy changed as a result of digital surveillance?
- How well do regional and international legal systems guard against modern forms of surveillance?
- In what ways do surveillance operations by the public and private sectors undermine current legal protections?

- What legislative changes are required to improve privacy protection in the digital era?

1.2. Research Objectives:

The following objectives are the focus of this study:

- Examine the theoretical underpinnings of digital surveillance and how it affects the right to privacy.
- Investigate how the legal notion of privacy has changed in response to technological developments.
- Assess how well regional and international legal frameworks safeguard privacy.
- Evaluate how private and public surveillance tactics affect fundamental rights.
- Determine the main practical and legal issues around digital surveillance.
- Suggest a more advanced legal strategy capable of addressing the complexities of modern surveillance technologies.

1.3. Methodology:

In order to give a thorough and in-depth investigation of the relationship between digital surveillance and the right to privacy and to evaluate the suitability of current legal frameworks in handling modern technological concerns, this study employs a number of methodological approaches.

- The doctrinal method is used to examine international and regional legal instruments, including treaties, conventions, and case law related to the right to privacy.
- The analytical method is used to evaluate these legal frameworks' suitability for dealing with contemporary surveillance techniques.
- The comparative approach is used to examine various surveillance governance models across different jurisdictions.

Additionally, the study maintains a strong focus on legal analysis and critical evaluation while incorporating a descriptive dimension to explain the conceptual and technological aspects of digital monitoring.

In order to distinguish various legislative approaches to surveillance governance and privacy protection, special attention is paid to comparative developments in the European Union, the United Kingdom, India, the United States, and China.

Section I: Conceptual Foundations of Digital Surveillance and the Right to Privacy:

We will address the following points in this section:

A) The Concept of Digital Surveillance:

1 - Definition of Digital Surveillance:

The term “Digital Surveillance” describes the methodical monitoring, gathering, analysis, and archiving of people's data using cutting-edge digital technology for governance, security, or control¹.

Closed-circuit television (CCTV), biometric identification systems, tracking software, and artificial intelligence are just a few of the many technological tools used in modern digital surveillance. These tools allow both state and non-state actors to monitor communications, analyse metadata, track physical movements, and perform extensive data mining of online activities².

Such actions raise grave concerns about the protection of fundamental human rights, particularly the right to privacy, freedom of expression, and freedom of association, even though they may have justifiable purposes, especially when it comes to public safety and national security³.

Because it makes it possible to continuously gather, process, and analyze vast amounts of personal data, digital surveillance is different from traditional monitoring from a legal standpoint. As a result, privacy issues are becoming more prevalent in data aggregation, profiling, and automated decision-making processes in addition to direct observation.

2- Types of Digital Surveillance:

Depending on its scope, actors, and technological instruments, digital surveillance can take many different forms. One of the most common types is biometric surveillance, which uses distinct biological identifiers including speech patterns, iris scans, fingerprints, and facial recognition to accurately identify people. These systems are being incorporated more and more into law enforcement procedures, border control systems, and national identification programs.

Facial recognition surveillance is another important type that is frequently used in public areas, airports, and urban settings. Although its use without informed consent and its acknowledged biases, especially along racial and gender lines, pose severe issues about discrimination and mistaken identification, it is frequently justified on security grounds⁴.

Furthermore, mass data surveillance is a ubiquitous type of monitoring that is based on the extensive gathering and examination of metadata and personal data produced by digital devices like smartphones, web browsers, and smart technologies. Large-scale initiatives like the NSA's PRISM program demonstrate how this type of surveillance facilitates the development of comprehensive behavioural profiles and helps predictive analytics⁵.

Moreover, another crucial aspect of digital monitoring is corporate surveillance, also known as "surveillance capitalism". This strategy raises issues with informed consent, data monopolies, and user behavior manipulation when private corporations gather and profit from user data for targeted advertising and behavioural prediction.

Lastly, the global deployment of surveillance technology, especially when outsourced to governments with lax legal protections, allows digital surveillance to transcend national borders and be utilized for political control and opposition suppression⁶.

The legal issue is not just that these types of monitoring use different tools; it is also that they interfere with people's rights in different ways and to varying degrees. Because biometric and facial recognition surveillance turn the human body into a permanent identifier and blur the line between identification and traceability, they are especially invasive. Contrarily, corporate spying shows that private organizations now have quasi-governing power through behavioural tracking and predictive analytics, proving that dangers to privacy no longer come solely from the state.

B) The Evolution of the Concept of Privacy:

1 - The Origins of the Concept of Privacy:

The modern concept of privacy is said to have originated with Louis Brandeis and Samuel Warren's well-known work "The Right to Privacy", which was published in 1890. This development was a crucial turning point⁷.

According to Warren and Brandeis, privacy needed to be acknowledged as a separate legal right that shields people from having their personal information disclosed without authorization. Their famous definition of privacy as "the right to be let alone" served as the cornerstone of contemporary privacy legislation and had a big impact on subsequent legal advancements⁸.

This signaled a profound change in legal philosophy since privacy was now seen as a defense of human individuality and individual autonomy rather than just in connection to property rights.

The acknowledgement of privacy as a protected legal interest separate from property rights is the legal significance of Warren and Brandeis' contributions. Later, this conceptual change had an impact on data protection, human rights, and constitutional frameworks in several legal systems.

While protection against revelation was the main focus of the traditional understanding of privacy, data collecting, automated processing, profiling, and algorithmic decision-making are now major sources of privacy issues. As a result, contemporary privacy law covers more comprehensive types of information protection in addition to secrecy.

2- The Conceptual Foundations of Privacy in the Age of Digital Surveillance:

The majority of modern legal study acknowledges privacy as a multifaceted term that encompasses information control, personal liberty, human dignity, and defense against undue intrusion. There is general consensus that contemporary privacy issues go beyond secrecy and include the gathering, processing, storing, and use of personal information in digital contexts, despite the fact that academics have taken differing stances when defining privacy⁹.

It seems challenging to create a comprehensive legal definition of privacy when it must be understood in the context of modern society and economic structures. The right to privacy is acknowledged in some international legal texts notwithstanding these difficulties. Nevertheless, “it is unclear how or even if effective legal protection can be provided when the target of the protection cannot be identified with certainty”¹⁰.

Beyond privacy itself, a variety of rights and freedoms, including equality, freedom of expression, freedom of association, and democratic participation, may be impacted by digital surveillance. Because of this, modern privacy protection is crucial to defending more general human rights concerns in digital society.

Section II: The International Legal Framework for Privacy Protection in the Face of Digital Surveillance:

We will address the following points in this section:

A) The International Legal Recognition of the Right to Privacy:

The right to privacy was recognized as a first-generation fundamental human right in numerous international legal instruments adopted in the second half of the twentieth century. While these instruments affirm the existence of the right, they generally do not provide a precise definition of privacy. Nevertheless, a wide range of international human rights agreements, at both global and regional levels, provide for its protection.

The Universal Declaration of Human Rights (UDHR) constitutes a foundational text in this regard. Article 12 states that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation,” and that everyone has the right to legal protection against such interference or attacks. Although the UDHR is not legally binding, it is widely regarded as part of customary international law and has served as an interpretative foundation for subsequent binding instruments¹¹.

This recognition is reinforced by Article 17 of the International Covenant on Civil and Political Rights (ICCPR) (1966), which prohibits arbitrary or unlawful interference with privacy and obliges States Parties to adopt legislative measures to give effect to this right¹². The Covenant thus

transforms the recognition of privacy into a binding legal obligation at the international level. Therefore, the primary universal legal foundation for assessing whether digital monitoring methods are compliant with international human rights law is Article 17. States Parties are subject to legally binding responsibilities under the ICCPR, in contrast to the UDHR, which offers a normative framework.

The ICCPR strengthens the legal protection of privacy on a global scale by imposing binding obligations on states parties, they are under a legal obligation to respect and ensure this right for all individuals within their territory and subject to their jurisdiction and to provide effective protection through domestic law.

The Human rights Committee, the treaty body supervising implementation of the ICCPR, has provided authoritative interpretation of article 17 in general comment no.16 (1988). The committee emphasized that protection against arbitrary or unlawful interference must extend to acts by both state authorities and private actors, and that states must enact legislative and other measures to give real effect to this right. In its concluding observations, the HRC has clarified that any interference with privacy must satisfy the principles of legality, necessity and proportionality to be compatible with article 17.

The committee has applied these standards to a wide range of issues, including surveillance measures, data retention. Its practice has become a central reference for assessing whether domestic laws and practices involving personal data processing or other intrusions into private life comply with UN human rights obligations¹³. Crucially, both positive and negative responsibilities are established by the Committee's judgment. In addition to adopting laws and regulations that can shield citizens against private actors' invasions of privacy, states must abstain from arbitrary interference with privacy.

The right to privacy is also reflected in specialized UN human rights treaties, including Article 16 of the Convention on the Rights of the Child and Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, which extend privacy protections to specific groups¹⁴.

At the regional level, Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life. It provides that everyone has the right to respect for their private and family life, home, and correspondence, while allowing public authorities to interfere with this right only where such interference is lawful, necessary in a democratic society, and justified by legitimate aims such as national security, public safety, or the protection of the rights and freedoms of others.

Article 8 is one of the most successful regional privacy protection regimes now in use since it offers both substantive protection for privacy and a judicial enforcement mechanism through the European Court of Human Rights.

B) Privacy Protection in the United Nations System:

The emergence of mass surveillance, bulk data collection, and digital technologies has prompted various organs of the United Nations, including United Nations General Assembly, The Office of the High Commissioner for Human Rights (OHCHR), and the United Nations Human rights Council (HRC), to develop a specific agenda on “the right to privacy in the digital age”.

Following revelations of extensive communications surveillance, the General Assembly adopted a series of resolutions, beginning with UN General Assembly Resolution 68/167. This resolution affirms that the same rights individuals enjoy offline must also be protected online, including the right to privacy. It calls upon states to review their legislation and practices, ensure that any interference with privacy is lawful and non-arbitrary, and establish effective oversight and remedies¹⁵.

The OHCHR has further elaborated this framework through its thematic reports on the right to privacy in the digital age. These reports emphasize that digital surveillance and data processing must comply with the principles of legality, necessity, and proportionality, and must be subject to independent and effective oversight mechanisms, as well as accessible remedies.

In 2015, the Human Rights Council established the mandate of the UN Special Rapporteur on the Right to Privacy to strengthen expertise and monitoring at the international level. The Special Rapporteur reports annually to both the Human Rights Council and the General Assembly on developments, challenges, and best practices in privacy protection, with particular attention to surveillance and data protection. The mandate includes examining alleged violations worldwide, formulating recommendations on domestic and international norms, and engaging in dialogue with States, international organizations, and private actors¹⁶.

In September 2019, the Human Rights Council adopted Human Rights Council Resolution 42/15, which recognizes that the development and deployment of new and emerging technologies can significantly affect the enjoyment of the right to privacy and other human rights. The resolution sets out a range of recommendations addressed to both States and business enterprises to ensure respect for privacy in the digital environment¹⁷.

While the UN framework on digital surveillance has significantly clarified States' human rights obligations, its effectiveness remains limited. Most General Assembly resolutions and thematic reports are non-binding and rely primarily on political persuasion rather than legal enforcement. As a result, compliance largely depends on States' willingness to implement reforms, and many continue to operate broad or opaque surveillance regimes that fall short of international standards.

Moreover, monitoring and follow-up mechanisms face structural constraints. Bodies such as special rapporteurs, treaty bodies, and the Universal Periodic Review can document and criticize violations but lack the authority to invalidate domestic laws or impose sanctions. This limitation weakens the practical impact of the framework. Therefore, the establishment of norms and standards is the fundamental strength of the UN system, while the lack of direct enforcement measures that can guarantee constant state compliance continues to be its main drawback¹⁸.

C) Privacy Protection in the European Regional System:

The right to respect for private and family life, home, and correspondence is guaranteed under article 8 of the 1950 European Convention on Human Rights (ECHR). While this provision allows for certain interferences by public authorities, such limitations must be justified as "necessary in a democratic society" for legitimate aims, including national security and public safety.

In interpreting this clause, the European Court of Human Rights (ECtHR) has developed a robust body of jurisprudence grounded in the principles of proportionality and judicial oversight, thereby seeking to strike a balance between individual privacy rights and state surveillance measures¹⁹. As a result, Article 8 has become a dynamic legal instrument for preserving privacy in the face of contemporary surveillance challenges.

Furthermore, The European Court of Human Rights has consistently stressed that the notion of “private life” is not exhaustive, allowing for a flexible and evolving interpretation that adapts social and technological developments. In particular, it has recognized the protection of personal information as an essential part of the right to privacy, especially in the context of modern surveillance practices²⁰. Through this evolving approach, the ECtHR has extended the scope of Article 8 to include digital communications, digital activities, and the processing of personal data, thereby reinforcing the applicability of Article 8 in the digital era.

The European model is often seen as the most sophisticated regional framework for handling privacy concerns originating from digital surveillance, and this jurisprudential evolution shows how Article 8 can be adjusted to technological progress. Despite its advantages, the European framework nevertheless has to deal with issues brought on by quickly developing surveillance technology, especially when it comes to large-scale cross-border data processing, artificial intelligence, and predictive analytics.

Section III: Digital Surveillance in International Practice: State and Private Actors:

We will address the following points in this section:

A) Government Digital Surveillance Models:

The application of monitoring in real-world situations emphasizes its crucial role in national security. The practical benefits of monitoring technologies in foreseeing dangers, reducing hazards, and guaranteeing public safety are demonstrated by case studies from multiple countries.

The identification and prevention of a terrorist plot in the UK is a noteworthy illustration of efficient monitoring. Technology is used throughout CONTEST, the UK's 2023 Strategy for Countering Terrorism, from data collection and detection to surveillance, communications, and analysis²¹. Authorities were able to monitor and apprehend suspects before their plan was carried out by using advanced surveillance technologies like facial recognition and data analytics.

In India, the use of mobile network tracking and closed-circuit television (CCTV) cameras proved crucial in solving high-profile crimes, such as the terror attacks in Mumbai in 2008. New surveillance-related regulations were introduced in India following the 26/11 attacks. In particular, Section 69 of the IT Act (The Information Technology Act) was added through an amendment in 2009. When it was “necessary or expedient” to do so in the interest of public order, national security....etc²². Section 69 granted authorities the authority to intercept, monitor, or decrypt any online information using any computer resource. These activities show how surveillance can increase situational awareness and produce actionable intelligence, enabling quick and effective reactions.

In order to combat cyber dangers, the use of surveillance technology has shown to be quite beneficial. Advanced cyber security monitoring systems have been used by nations like the US to detect and prevent attacks on critical infrastructure. These protections ensure the continuance of essential services and protect sensitive data from cyberattacks. These instances show how monitoring can be used to address both digital and physical security concerns.

Legally speaking, the main question is not whether monitoring advances security goals but rather if the surveillance methods used adhere to relevant legal protections, such as need, legality, proportionality, and efficient oversight.

However, there is debate around these accomplishments. China's widespread use of surveillance, exemplified by the Social Credit System, has been criticized for its intrusive features and its potential use to suppress dissent. By gathering social credit data from every person and business, the system will serve as a national incentive system to reward behaviors that uphold trust and penalize those that do not²³. This raises important questions about the morality of surveillance

and how it affects personal freedoms. The deployment of monitoring devices often sparks public debate about the extent to which privacy may be compromised for security reasons in democracies.

Surveillance does not function in a neutral political vacuum, as demonstrated by comparative state practice. Depending on the legal and constitutional framework, the same technologies may serve significantly different purposes. In authoritarian contexts, Surveillance may become a tool of social control and political conformity, whereas in democratic systems, it is at least officially limited by legality and scrutiny. As a result, the institutional environment in which surveillance is embedded must be taken into consideration while evaluating its legality rather than focusing solely on its technical design.

The comparative instances show that the legality of monitoring depends not only on the technology used but also on the presence of unambiguous laws, judicial approval, impartial oversight, and efficient safeguards against misuse.

B) Digital Surveillance in the Private Sector:

Traditional means of tracking persons or locations are no longer the only way to conduct surveillance. It has spread into the digital sphere, where private sector businesses employ it to consistently and methodically track communications, actions, and habits. Private businesses are now able to gather, process, and analyze previously unheard-of amounts of personal data because of technological advancements. As a result, surveillance now encompasses more behavioral analysis, profiling, and predictive data processing in addition to traditional security duties²⁴.

Social media platforms, which generate massive volumes of data every day from posts, comments, likes, shares, searches, and even the duration of user interaction, are where the significance of this shift is most noticeable. In addition to being gathered for business, this data is now crucial for security and surveillance analysis. Data analytics and artificial intelligence tools allow for the tracking of general trends, the detection of anomalous behaviors, the analysis of interpersonal networks, and the identification of themes that cause conflict or social engagement. Because social media platforms enable the compilation of a nearly comprehensive profile of individuals and organizations, including their interests, trends, locations, and communication habits, they have become a fertile ground for digital surveillance²⁵.

The risk associated with this position stems from the fact that data analysis on these platforms goes beyond simple observation to create comprehensive digital profiles of individuals, which enable behavior prediction, classification, or influence. Here, digital surveillance evolves from simple monitoring into an analysis, inference, and manipulation-based technique that raises significant ethical and legal concerns about privacy, transparency, and the boundaries of the use of personal data. Additionally, because this surveillance is ongoing and frequently undetectable, people are constantly under observation without fully understanding the volume of information gathered about them or how it is put to use²⁶.

These advancements highlight the increasing demand for legal frameworks that can control algorithmic decision-making, profiling, and data gathering while maintaining lawful business operations.

One of the most significant changes in modern privacy law is illustrated by private-sector surveillance: the shift from state-centered intrusion to market-based monitoring. Corporate data extraction frequently relies on contractual opacity, default consent mechanisms, and behavioral nudging rather than overt coercion, in contrast to traditional surveillance techniques. This does not make it any less intrusive; in fact, because it is accepted through regular use of digital services, it can be more challenging to resist. The legal ramifications are obvious: where consent is technically

manipulated, monetarily conditioned, or structurally uninformed, it can no longer serve as a sufficient barrier for privacy protection.

C) The Transnational Nature of Digital Surveillance:

By enabling quick data transfers, low-latency communication, and pervasive device interoperability, the combination of 5G networks with Internet of Things (IoT) technologies has completely transformed the global cyberspace. This generation's technological advancement has increased the capacity for cross-border surveillance, which could have a serious negative effect on people's right to privacy²⁷.

Both state and non-state actors can implement the 5G/IoT-led cross-border surveillance system, and they can penetrate and carry out cross-border surveillance using network slicing, edge computing, or ubiquitous sensors. These actions would result in a violation of established legal protections, leading to regulatory gaps and jurisdictional flaws. Through unique identifiers (such as IMSI), 5G and IoT enable granular user tracking, exposing people to identity-based surveillance²⁸. When IoT devices increase this danger by gathering real-time physiological and behavioral data, it gets even worse.

When it comes to resolving the privacy concerns of international data transfers and cross-border surveillance, judicial practice has been especially significant. Through numerous case rulings, mostly from European courts, the doctrine pertaining to cross-border monitoring and the right to privacy has evolved. The following are some of these significant cases and how they have strengthened the right to digital privacy:

- **Schrems I (2015):** Mr. Maxmillian Schrems, an Austrian privacy advocate, filed a complaint against Facebook Ireland in 2015. He contested the legitimacy of the EU-US Safe Harbour Agreement, which allowed data transfers to the US. This arrangement gave the US access to user data transfers without sufficient safeguards, resulting in the compromise of EU citizens' data. According to the Court of Justice of the European Union (CJEU), the Safe Harbour Agreement gave US intelligence agencies unjustified and excessive access to the data of EU residents. As a result, the CJEU ruled that the Safe Harbour Agreement was unconstitutional because it violated EU residents' right to privacy²⁹.

This jurisprudential reform was the first of its kind as it safeguarded data privacy from cross-border and widespread surveillance by foreign intelligence agencies such as those of the United States.

- **Schrems II (2020):** The EU-US Privacy Shield was created to offer a new framework for data transmission following the invalidation of the Safe Harbour Agreement. Schrems also contested this new framework on the same grounds used in the earlier case, namely that it did not provide sufficient protections for EU citizens' right to privacy. The CJEU noted that US intelligence services had access to the personal data of EU nationals under Section 702 of the Foreign Intelligence Surveillance Act (FISA). The Court emphasized that before sending data to third countries, Data Transfer Impact Assessment (DTIA) must be carried out. It further held that, to ensure adequate protection of EU citizens' data, a comprehensive assessment of third-country legal frameworks is required. Ultimately, the Court invalidated the EU-US Privacy Shield framework on the grounds that it did not provide sufficient safeguards for EU citizens' right to privacy³⁰.
- **UK v. Big Brother Watch:** The European Court of Human Rights (ECtHR) was considering the UK's widespread surveillance system in the Big Brother Watch v. UK case. Through mass surveillance operation, the UK collected a significant amount of personal data—including metadata—without individuals' consent. The Court held that because the UK's mass surveillance program lacked sufficient safeguards, it breached people's right to privacy. According to the Court,

surveillance measures could be carried out in exceptional situations when strict necessity and reasonable suspicion are essential prerequisites. Accordingly, indiscriminate or insufficiently supervised mass surveillance may breach Article 8 of the ECHR³¹.

- **Puttaswamy v. Union of India (2017):** Justice K.S. Puttaswamy, a retired High Court judge, filed a petition in 2012 challenging the constitutionality of the "Aadhaar Program," which required biometric identification in order to gather personal information (such as fingerprints and iris scans) to collect personal data for the purpose of delivering welfare benefits. The government defended the Aadhaar program by arguing that privacy was not a basic right, relying on the decisions in *M.P. Sharma* (1954) and *Kharak Singh* (1962), which had upheld the constitutionality of invasive police surveillance and warrantless searches conducted under colonial-era laws. The Supreme Court of India redefined privacy and overruled earlier judicial decisions from the colonial past. The Court clarified that individual autonomy, dignity, and informational self-determination all depend on privacy. The court held that Articles 14, 19, and 21 of the Indian Constitution protect privacy as a fundamental constitutional human right. Following this landmark judgment, The Digital Personal Data Protection Act (DPDPA) 2023 was enacted, it was the India's first comprehensive data protection legal framework. The Act established a Data Protection Board (DPD) to oversee enforcement procedures, requires user consent for data collecting, and provides for significant penalties for data breaches. In the context of increasing algorithmic governance, cross-border data flows, and AI-driven systems, this ruling significantly reshaped the understanding of digital rights³².

These court rulings demonstrate the increasing understanding that privacy protection has to transcend national boundaries. They also highlight the shortcomings of disjointed legal frameworks and the growing demand for global norms that can control cross-border data transfers and monitoring operations.

Section IV: Legal and Practical Challenges in Digital Surveillance:

We will address the following points in this section:

A) The Dilemma of Balancing Security and Privacy:

One of the main legal issues with modern surveillance legislation is the connection between security and privacy. International human rights law does not forbid monitoring in and of itself; rather, it mandates that surveillance actions have a justifiable purpose and adhere to the standards of legality, need, proportionality, and efficient oversight³³.

In this sense, applying the principles of necessity and proportionality in the context of digital monitoring has become a significant challenge. According to these principles, any interference with privacy must be limited to what is strictly necessary and proportionate, and it must be justified by a legitimate aim. However, contemporary surveillance technologies often operate in a preventive and broad manner, frequently lacking individualized suspicion, especially those based on large-scale data collection and algorithmic analysis. This calls into question the effectiveness of these principles as protection for digital privacy by raising doubts as to whether such methods can satisfy the requirements of necessity and proportionality.

Therefore, privacy shouldn't just be seen as a barrier to security measures. Instead, it is a crucial part of democratic governance and the rule of law, necessitating that surveillance capabilities continue to be subject to significant legal constraints.

B) Technological Challenges:

The breadth and capacities of contemporary surveillance and data processing systems have been greatly enlarged by rapid technical advancements, particularly in the areas of artificial intelligence and the Internet of Things (IoT). These technologies present significant hazards to

individual privacy even as they offer increased efficiency and new options for cybersecurity and data analysis. AI systems' capacity to handle enormous volumes of data makes it easier to engage in activities like automated decision-making and non-consensual profiling, which are frequently accompanied by algorithmic bias and a lack of transparency³⁴.

Large-scale crises like those involving Facebook and Equifax demonstrate how the growing reliance on digital infrastructures has increased vulnerability to data breaches and cyber threats. These breaches expose serious flaws in information security and data protection systems, eroding public confidence and putting people and businesses at serious risk of identity theft, monetary loss, and reputational injury³⁵.

As a result, even though technology improvements are advantageous, they have also created a complicated risk environment that puts privacy protection at risk and necessitates more robust technical, ethical, and regulatory protections.

Because algorithmic systems sometimes use opaque decision-making procedures, artificial intelligence presents extra-legal concerns. Courts, regulators, and impacted parties may find it more difficult to comprehend, contest, or review decisions pertaining to surveillance as a result.

Therefore, systems that guarantee algorithmic transparency, explainability, independent auditing, and efficient regulatory oversight are necessary for modern privacy protection. Legal protections run the risk of being challenging to implement in reality in the absence of such safeguards.

Section V: Towards a Sophisticated International Legal Framework for Digital Governance:

We will address the following points in this section:

A) Strengthening Legal Safeguards in Digital Surveillance:

A legislative framework based on four fundamental principles—legality, necessity, proportionality, and accountability—is necessary for the effective regulation of digital surveillance. Under international human rights law, these principles offer the main legal criteria by which surveillance practices should be assessed.

Any interference with the right to privacy must have a transparent and easily accessible legal foundation, according to the legal principle. Secret executive orders or administrative discretion should not be the foundation for surveillance measures, nor should they be based on ambiguous or unduly expansive regulations. Laws permitting surveillance must be open to frequent public examination and democratic debate, and they must clearly describe the scope, purpose, and boundaries of the surveillance. Legislative transparency is essential because it makes it clear to the public what types of surveillance are allowed, by whom, under what circumstances, and with what protections³⁶.

According to the concept of need, surveillance must only be carried out for justifiable purposes that are acknowledged by human rights legislation, such as public safety, national security, or crime prevention. Surveillance should not be the first course of action, even in situations where such goals are present. States must show that the particular measure is strictly essential to accomplish the declared goal and that less invasive options have been explored and determined to be insufficient.

This rule prohibits governments from using general excuses to carry out preventive or indiscriminate surveillance without specific suspicion. A crucial balancing test between individual rights and group interests is the proportionality concept. It requires that any intrusion into privacy be proportionate to the objective pursued, meaning that the benefits of surveillance must outweigh the harm to individual rights and freedoms. The extent of data acquired, the sensitivity of the material, the length of monitoring, and the possibility of abuse or exploitation must all be considered in

proportionality evaluations. For instance, indiscriminate mass surveillance programs or general data retention rules are unlikely to satisfy the proportionality requirement, particularly if they lack specific grounds³⁷.

In order to prevent the misuse of surveillance powers and to guarantee that individuals have access to effective remedies when their rights are violated, accountability mechanisms are crucial.

Oversight bodies must be independent, adequately resourced, and empowered to review surveillance activities, audit intelligence operations, and investigate complaints. Intrusive kinds of surveillance should require judicial authorization, and in situations where real-time judicial approval is not practical, ex post facto review must be available. By illuminating the scope and character of monitoring techniques, public reporting requirements like transparency reports and parliamentary briefings help improve accountability³⁸. Data protection principles, such as purpose limitation, data minimization, storage limitation, integrity, confidentiality, and user control, must also be given top priority in a human rights framework. Comprehensive data protection legislation like the European Union's General Data Protection Regulation (GDPR) as well as an increasing number of national laws worldwide reflect these principles. A strategy known as "privacy by design" requires surveillance systems to be created with privacy considerations integrated from the outset, incorporating robust safeguards to protect data against breaches, unauthorised access, and secondary use.

Highly intrusive monitoring methods should typically require prior judicial authorization in addition to these protections. In addition to helping to ensure that surveillance powers are only used when absolutely justified by legitimate aims and supported by adequate evidence, judicial review is a crucial safeguard against arbitrary interference with privacy.

Artificial intelligence-based surveillance technologies should also receive special consideration. To ensure compliance with human rights standards and prevent discriminatory outcomes, regulatory frameworks should mandate transparency, explainability, and frequent independent audits because algorithmic monitoring may involve automated profiling, behavioral prediction, and opaque decision-making processes.

Additionally, technology businesses must to be held to higher standards of accountability. Transparency reporting, human rights impact assessments, data minimization standards, and efficient channels for people to contest illegal data collecting, processing, and profiling activities are some examples of such obligations.

Protecting marginalized and vulnerable groups—who are frequently disproportionately impacted by surveillance—is another essential component of a human rights-based approach. Religious minorities, journalists, political dissidents, migrants, and economically disadvantaged communities are frequently subjected to heightened surveillance, often without sufficient justification. Therefore, anti-discrimination safeguards, prohibitions on racial, religious, or political profiling, and guarantees that surveillance is not used as a tool to suppress dissent or influence electoral processes are all essential elements of a rights-respecting framework.

Furthermore, a thorough framework must expand regulatory control to the private sector in a world where private actors—such as technology corporations, telecom providers, and data brokers—conduct a large amount of surveillance. States have an obligation not only to respect individuals' rights but also to protect them from third-party abuses. This includes requiring companies to implement robust encryption standards, publish transparency reports, disclose surveillance requests, and challenge unwarranted government access requests³⁹.

In an increasingly linked digital world, international collaboration is also essential for controlling surveillance. Harmonized legal norms and shared commitments to respect human rights

obligations are necessary for regulating cross-border data flows, intelligence-sharing agreements, and cooperative surveillance operations.

Multilateral agreements like the United Nations Guiding Principles on Business and Human Rights and the Council of Europe's Convention 108+ provide important guidance for the development of international norms on responsible surveillance governance. A rights-based regulatory framework helps guarantee that surveillance technologies continue to be compatible with individual liberties, democratic principles, and globally accepted human rights norms.

B) Global Governance of Digital Surveillance:

Because data flows, surveillance technology, and algorithmic systems frequently operate across borders, the transnational character of digital surveillance poses a fundamental challenge to the efficacy of national legal regimes. Since no state can successfully monitor or manage surveillance tactics in this situation on its own, international collaboration is a necessity rather than a choice of policy. Different national standards compromise privacy protection and allow for regulatory arbitrage as a result of the globalization of data processing, which is fueled by international technology businesses and cross-border intelligence cooperation.

Accordingly, the harmonization of privacy standards through bilateral agreements, multilateral frameworks, and adherence to international human rights principles has become increasingly necessary. Initiatives such as the OECD Privacy Guidelines and emerging efforts to establish international governance frameworks for artificial intelligence reflect attempts to bridge these regulatory gaps. However, such efforts often face limitations due to their non-binding nature and the lack of effective enforcement mechanisms. This raises critical concerns about the adequacy of international law in addressing digital surveillance, particularly in ensuring that fundamental principles such as necessity and proportionality are consistently applied across jurisdictions. Consequently, strengthening international cooperation is not only essential for regulatory alignment, but also for safeguarding privacy in an increasingly interconnected and technologically driven world⁴⁰.

Despite these efforts, there are still large gaps in the protection of privacy around the world due to the lack of a comprehensive and legally binding international instrument that particularly regulates digital monitoring.

A key component of guaranteeing accountability in the context of digital monitoring is the creation of independent oversight agencies, especially data protection authorities, in tandem with the requirement for international collaboration. Traditional methods of oversight are frequently inadequate due to the complexity and opacity of contemporary surveillance technologies, particularly those based on artificial intelligence and algorithmic decision-making. By continuously monitoring both state and private surveillance techniques, independent authorities—equipped with sufficient legal mandates, financial resources, and technical know-how—play a critical role in closing this gap.

These organizations must have the power to look into surveillance systems, carry out algorithmic audits, and evaluate adherence to human rights and data protection regulations, including proportionality and need. Furthermore, in order to prevent abuses and guarantee effective enforcement, their capacity to apply penalties and corrective actions is crucial. Surveillance operations run the risk of operating in a regulatory vacuum without such independent scrutiny, which is marked by a lack of accountability, a lack of transparency, and an increased risk of human rights breaches. As a result, establishing independent regulatory bodies is essential for preserving public confidence and safeguarding privacy in the digital era, rather than only serving as a governance instrument⁴¹.

Conclusion:

The study's analysis shows that the structure and purpose of surveillance practices in modern society have undergone a significant change as a result of digital surveillance. In contrast to classical surveillance, which was typically limited, targeted, and reactive, modern digital surveillance operates through continuous, large-scale, and predictive methods that fundamentally alter the relationship between individuals, states, and private actors.

Simultaneously, the evolution of the right to privacy—from the traditional notion of the “right to be let alone” to a more complex framework focused on informational control—reflects the increasing impact of technological advancements on legal concepts. Although privacy has been formally recognized as a fundamental human right in international and regional legal frameworks, this study demonstrates that such recognition remains largely normative and insufficient in practice.

The results show a structural disconnect between current legal frameworks and rapidly evolving surveillance technologies. Even though they are fundamental, principles such as necessity, proportionality, and legality become increasingly difficult to apply to global, algorithm-driven, and systemically integrated forms of monitoring. Furthermore, the effectiveness of conventional state-centered regulation strategies is further undermined by the expansion of private sector surveillance and cross-border data flows. The case law examined -from Schrems I and II to Big Brother Watch and Puttaswamy- confirms that courts are beginning to adapt traditional concepts of privacy and data protection to the realities of mass and transnational surveillance, but also illustrates the limits of fragmented and regionally bounded approaches.

The study also concludes that although current legal frameworks offer significant privacy protections, they are still inadequate to handle new issues related to corporate surveillance, artificial intelligence-driven monitoring, large-scale data processing, and international data transfers. These developments highlight the need for more flexible and efficient legal responses and reveal significant regulatory flaws.

As a result, enhancing privacy protection in the digital world necessitates a number of complementary actions. Strengthening judicial oversight of intrusive surveillance measures, guaranteeing accountability and transparency in AI-based monitoring systems, enforcing stricter regulations on technology companies, and encouraging global collaboration in the governance of cross-border surveillance practices are all indispensable measures if digital surveillance is to remain compatible with democratic values and the rule of law.

Future legal reforms should specifically concentrate on establishing independent data protection authorities, requiring prior judicial authorization for highly intrusive surveillance measures, requiring technology companies to be transparent, and creating legally binding international standards governing data transfers and cross-border surveillance.

Citations:

¹ David Lyon, *Surveillance Studies an Overview*, Polity Press, 2007, PP. 11- 46.

² Leith Jeroudi, *Surveillance and Human Rights*, Geneva Centre for Human Rights Advancement and Global Dialogue, June 2023, available at: <https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf>.

³ United Nations, Human Rights Council, *The Right to Privacy in the Digital Age*, 2022, Available at: <https://digitallibrary.un.org/record/3985679?v=pdf#files>.

⁴ Aashi Dixit, *Digital Surveillance and the Right to Privacy: Reassessing Human Rights in the Age of Technology*, *Indian Journal of Integrated Research in Law*, Vol. V, Issue V, 2025, PP. 122- 124.

- ⁵ Daniel J. Solove and Paul M. Schwartz, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, GW Law Faculty Publications & Others Works, Vol. 86, 2011, PP. 1814-1828.
- ⁶ Dixit, Op, Cit, PP. 122- 124.
- ⁷ Milton R. Konvitz, Privacy and the Law: A Philosophical Prelude, Law and Contemporary Problems, Vol. 31, Issue 2, 1996, PP. 1- 9.
- ⁸ Benjamin E. Bratman, Brandeis and Warren's the Right to Privacy, Tennessee Law Review, Vol. 69, 2002, PP. 623- 625.
- ⁹ T. Gerety, Redefining Privacy, Harvard Civil Rights- Civil Liberties Law Review, Vol. 12, Issue 2, 1977, P. 281.
- ¹⁰ Robert C. Post, Three Concepts of Privacy, The Georgetown Law Journal, Vol. 89, 2001, PP. 2087-2098.
- ¹¹ Article 12 of the Universal Declaration of Human Rights, 1948.
- ¹² Article 17 of the International Covenant on Civil and Political Rights, 1966.
- ¹³ General Comment No.16 : Article 17 (the Right respect of privacy, family, home and correspondence and protection of Honour and Reputation), human rights committee, thirty -second session, adopted 08 April 1998, Office of the High Commissioner for Human rights, HRI/GEN/1/Rev.9 (vol.1), available on: <https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf>
- ¹⁴ Privacy: What It Is And Why It Is Important, Office on Drugs and Crime, United Nations, available on :<https://www.unodc.org/cld/pt/education/tertiary/cybercrime/module-10/key-issues/privacy-what-it-is-and-why-it-is-important.html>
- ¹⁵ New UN Resolution amplifies call for right to privacy in the light of mass surveillance, CCDCOE, available on: <https://ccdcoe.org/incyber-articles/new-un-resolution-amplifies-call-for-right-to-privacy-in-the-light-of-mass-surveillance/>
- ¹⁶ How to talk about the Right to Privacy at the UN, a brief guide, privacy international , March 2017, pp 6-8, available on: https://privacyinternational.org/sites/default/files/2017-12/UN_Guide_Final.pdf
- ¹⁷ International Standards, OHCHR and privacy in digital age, United Nations Human Rights office of the High Commissioner, United Nations, available on: <https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards>
- ¹⁸ for more details, see: Surveillance And Human Rights, Report of The Special Rapporteur on The Promotion and Protection of the Right To Freedom of Opinion and Expression, Human Rights Council, 41 session, 24 june-12 july 2019, A/HRC/41/35, available on: <https://docs.un.org/en/A/HRC/41/35>
- ¹⁹ Article 8 of the European Convention on Human Rights (ECHR), 1950.
- ²⁰ Kristian P Humble, International law, surveillance and the protection of privacy, the international journal of human rights, Vol. 25 Issue 1, 2021, P. 4.
- ²¹ U.K. Home Office, Counter-Terrorism Strategy (CONTEST) 2023 (Accessible), Policy Paper, 2023, Available at: <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023/counter-terrorism-strategy-contest-2023-accessible>.
- ²² Anushka Jain and Vrinda Bhandari, The Development of Surveillance Technology in India: Beyond Judicial Review Or Oversight, VerfBlog, 2022, Available at: <https://verfassungsblog.de/os6-india/>.
- ²³ Eunsun Cho, The Social Credit System: Not Just Another Chinese Idiosyncrasy, Journal of Public & International Affairs, 2020, Available at: <https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy>.
- ²⁴ Mahamudul Hasan and Yousef Sheikh Salahuddin, Marketing of Security and Surveillance Products, Advances in Management, Vol. 12, Issue 3, 2019, PP. 36- 42.

- ²⁵ Shoshana Zuboff, Big other: Surveillance Capitalism and the Prospects of an Information Civilization, *Journal of Information Technology*, Vol, 30, 2015, PP. 75- 89.
- ²⁶ Mahamudul Hasan and Yousef Sheikh Salahuddin, Marketing of Security and Surveillance Products, *Ibid*, PP. 36- 42.
- ²⁷ Dan Wang, Dong Chen, Bin Song, Nadra Guizani, Xiaoyan Yu, and Xiaojiang Du, From IoT to 5G IIoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies, *IEEE Communications Magazine*, Vol. 56, Issue 10, 2018, PP. 114- 120.
- ²⁸ Muhammad, Khan, Tanveer Hussain, Joel J. P. C. Rodrigues, Paolo Bellavista, Antonio Roberto L. De Macedo, and Victor Hugo C. De Albuquerque, Efficient and Privacy Preserving Video Transmission in 5G-Enabled IoT Surveillance Networks: Current Challenges and Future Directions, *IEEE Network*, Vol. 35, Issue 2, 2021, PP. 26- 33.
- ²⁹ Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, Court of Justice of the European Union, October 2015, Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362>.
- ³⁰ Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, Court of Justice of the European Union, July 2020, Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311>.
- ³¹ Case of Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, May 2021, Available at: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%5D%7D>.
- ³² Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Writ Petition (Civil) No. 494 of 2012 (India), Available at: <https://indiankanoon.org/doc/91938676/>.
- ³³ Danial J. Power, Ciara Heavin and Yvonne o' Connor, Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide, *Journal of Business Analytics*, Vol. 4, Issue 2, 2021, PP. 155- 170.
- ³⁴ Anvesh Gunuganti, Privacy and Data Protection in the Digital Age, *Journal of Scientific and Engineering Research*, Vol. 5, Issue 12, 2018, P. 363.
- ³⁵ *Ibid*, P. 364.
- ³⁶ Aashi Dixit, Digital Surveillance and the Right to Privacy: Reassessing Human Rights in the Age of Technology, *Op, Cit*, PP. 129- 131.
- ³⁷ Office of the Privacy Commissioner of Canada, Exploring Facial Recognition Technology and its Impacts on Privacy, 2020, Available at: <https://www.priv.gc.ca/en/>.
- ³⁸ Benjamin Wittes and Jodie C. Liu, The Privacy Paradox: The Privacy Benefits of Privacy Threats, Center for Technology Innovation at Brookings, May 2015, PP. 3- 10.
- ³⁹ Alec Samuels, Legal Comment: No Tort Invasion of Privacy, *Mountbatten Journal of Legal Studies*, Vol. 7, Issu 1,2, 2003, PP. 75- 78.
- ⁴⁰ Oyedokun Godwin Emmanuel, Babalola Wasiu Adeyemo and Sakpere Wilson, Balancing Surveillance and Privacy: Legal Frameworks Governing Technology In The Digital Age, *Rivers State University Journal of Public Law*, Vol. 13, Issue 1, 2025, P. 224.
- ⁴¹ Hiroshi Tanaka, Zhang Wei and Zola Makatini, Digital Surveillance and the Erosion of Privacy: Legal Challenges in the Age of Artificial Intelligence, *American Journal of Law and Human Rights*, Vol. 1, Issue 1, 2025, PP. 19- 20.

Bibliography:

A- Books:

-David Lyon, *Surveillance Studies an Overview*, Polity Press, 2007.

B – Academic Articles:

-Aashi Dixit, *Digital Surveillance and the Right to Privacy: Reassessing Human Rights in the Age of Technology*, *Indian Journal of Integrated Research in Law*, Vol. V, Issue V, 2025.

-Alec Samuels, *Legal Comment: No Tort Invasion of Privacy*, *Mountbatten Journal of Legal Studies*, Vol. 7, Issue 1,2, 2003.

-Anvesh Gunuganti, *Privacy and Data Protection in the Digital Age*, *Journal of Scientific and Engineering Research*, Vol. 5, Issue 12, 2018.

-Benjamin E. Bratman, *Brandeis and Warren's , the Right to Privacy*, *Tennessee Law Review*, Vol. 69, 2002.

-Benjamin Wittes and Jodie C. Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, Center for Technology Innovation at Brookings, May 2015.

-Dan Wang, Dong Chen, Bin Song, Nadra Guizani, Xiaoyan Yu, and Xiaojiang Du, *From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies*, *IEEE Communications Magazine*, Vol. 56, Issue 10, 2018.

-Danial J. Power, Ciara Heavin and Yvonne o' Connor, *Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide*, *Journal of Business Analytics*, Vol. 4, Issue 2, 2021.

-Daniel J. Solove and Paul M. Schwartz, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, *George Washington Law Faculty Publications & Others Works*, Vol. 86, 2011.

-Hiroshi Tanaka, Zhang Wei and Zola Makatini, *Digital Surveillance and the Erosion of Privacy: Legal Challenges in the Age of Artificial Intelligence*, *American Journal of Law and Human Rights*, Vol. 1, Issue 1, 2025.

-Kristian P Humble, *International law, surveillance and the protection of privacy*, *the international journal of human rights*, Vol. 25 Issue 1, 2021

-Mahamudul Hasan and Yousef Sheikh Salahuddin, *Marketing of Security and Surveillance Products*, *Advances in Management*, Vol. 12, Issue 3, 2019.

-Milton R. Konvitz, *Privacy and the Law: A Philosophical Prelude*, *Law and Contemporary Problems*, Vol. 31, Issue 2, 1996.

-Muhammad, Khan, Tanveer Hussain, Joel J. P. C. Rodrigues, Paolo Bellavista, Antonio Roberto L. De Macedo, and Victor Hugo C. De Albuquerque, *Efficient and Privacy Preserving Video Transmission in 5G-Enabled IoT Surveillance Networks: Current Challenges and Future Directions*, *IEEE Network*, Vol. 35, Issue 2, 2021.

-Oyedokun Godwin Emmanuel, Babalola Wasiu Adeyemo and Sakpere Wilson, *Balancing Surveillance and Privacy: Legal Frameworks Governing Technology In The Digital Age*, *Rivers State University Journal of Public Law*, Vol. 13, Issue 1, 2025.

-Robert C. Post, *Three Concepts of Privacy*, *The Georgetown Law Journal*, Vol. 89, 2001.

-Shoshana Zuboff, *Big other: Surveillance Capitalism and the Prospects of an Information Civilization*, *Journal of Information Technology*, Vol, 30, 2015.

-T. Gerety, *Redefining Privacy*, *Harvard Civil Rights- Civil Liberties Law Review*, Vol. 12, Issue 2, 1977.

C - Websites:

-Anushka Jain and Vrinda Bhandari, *The Development of Surveillance Technology in India: Beyond Judicial Review Or Oversight*, *VerfBlog*, 2022, Available at: <https://verfassungsblog.de/os6-india/>.

- Case of Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, May 2021, Available at: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-210077%22%5D%7D>.
- Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/18, Court of Justice of the European Union, July 2020, Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311>
- Eunsun Cho, The Social Credit System: Not Just Another Chinese Idiosyncrasy, Journal of Public & International Affairs, 2020, Available at: <https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy>
- General Comment No.16 : Article 17 (the Right respect of privacy, family, home and correspondence and protection of Honour and Reputation), human rights committee, thirty -second session, adopted 08 April 1998, Office of the High Commissioner for Human rights, HRI/GEN/1/Rev.9 (vol.1), available on: <https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf>
- Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Writ Petition (Civil) No. 494 of 2012 (India), Available at: <https://indiankanoon.org/doc/91938676/>
- How to talk about the Right to Privacy at the UN, a brief guide, privacy international , March 2017, pp 6-8, available on: https://privacyinternational.org/sites/default/files/2017-12/UN_Guide_Final.pdf
- International Standards, OHCHR and privacy in digital age, United Nations Human Rights office of the High Commissioner, United Nations, available on: <https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards>
- Leith Jeroudi, Surveillance and Human Rights, Geneva Centre for Human Rights Advancement and Global Dialogue, June 2023, available at: <https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf>
- Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, Court of Justice of the European Union, October 2015, Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362>
- Office of the Privacy Commissioner of Canada, Exploring Facial Recognition Technology and its Impacts on Privacy, 2020, Available at: <https://www.priv.gc.ca/en/>
- New UN Resolution amplifies call for right to privacy in the light of mass surveillance, CCDCOE, available on: <https://ccdcoe.org/incyder-articles/new-un-resolution-amplifies-call-for-right-to-privacy-in-the-light-of-mass-surveillance/>
- Privacy: What It Is And Why It Is Important, Office on Drugs and Crime, United Nations, available on :<https://www.unodc.org/cld/pt/education/tertiary/cybercrime/module-10/key-issues/privacy-what-it-is-and-why-it-is-important.html>
- U.K. Home Office, Counter-Terrorism Strategy (CONTEST) 2023 (Accessible), Policy Paper, 2023, Available at: <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023/counter-terrorism-strategy-contest-2023-accessible>
- United Nations, Human Rights Council, The Right to Privacy in the Digital Age, report of the Office of the United Nations High Commissioner for Human Rights, 2022, Available at: <https://digitallibrary.un.org/record/3985679?v=pdf#files>.
- Surveillance And Human Rights, Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression, Human Rights Council, 41 session, 24 june-12 july 2019, A/HRC/41/35, available on: <https://docs.un.org/en/A/HRC/41/35>