تقنيات المراقبة وحقوق الإنسان: الموازنة بين الأمن والحرية

م.د. نيشتمان عثمان محمد

باحثة في مركز كردستان للوثائق والدراسات الأكاديمية ، جامعة السليمانية

إقليم كردستان العراق

البريد الإلكتروني Email : nishtiman.mohammed@univsul.edu.iq

الكلمات المفتاحية: المراقبة، حقوق الإنسان، الخصوصية، الذكاء الاصطناعي، الأمن القومي، التناسب.

كيفية اقتباس البحث

محمد ، نيشتمان عثمان ، تقنيات المراقبة وحقوق الإنسان: الموازنة بين الأمن والحرية،مجلة مركز بابل للدراسات الانسانية، كانون الثاني 2026،المجلد:16 ،العدد:1.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Surveillance Technologies and Human Rights: Balancing Security and Freedom

Dr. Nishtiman Othman Mohammed
Researcher at the Kurdistan Center for Documentation and Academic /Research, University of Sulaimani
Kurdistan Region of Iraq

Keywords : Surveillance, Human Rights, Privacy, Artificial Intelligence, National Security, Proportionality.

How To Cite This Article
Mohammed, Nishtiman Othman, Surveillance Technologies and Human Rights: Balancing Security and Freedom ,Journal Of Babylon Center For Humanities Studies, January 2026,Volume:16,Issue 1.

الملخص

لقد أحدث التقدّم السريع في تقنيات المراقبة الرقمية تحولًا جوهريًا في العلاقة بين أمن الدولة وحماية الحقوق الفردية. ومع الانتشار الواسع لاستخدام أنظمة التعرف البيومتري، والذكاء الاصطناعي، وتحليل البيانات على نطاق واسع، أصبحت المراقبة سمة مركزية للحكم المعاصر، في الوقت الذي تثير فيه تحديات قانونية وحقوقية عميقة. يتناول هذا البحث كيفية تقاطع ممارسات المراقبة مع مبادئ الخصوصية والحرية والمساءلة المنصوص عليها في الصكوك الدولية، مثل الإعلان العالمي لحقوق الإنسان (UDHR) والعهد الدولي الخاص بالحقوق المدنية والسياسية.(ICCPR)

من خلا أ ستخدام منهج نوعي وتأصيلي، يحلّل البحث المعاهدات الدولية والأعمال الأكاديمية والأطر السياسية لتقييم كيفية تبرير الدول وتنظيمها للمراقبة باسم الأمن القومي. كما يتبنى منظورًا مقارنًا لدراسة الاختلافات في المعايير القانونية وآليات الرقابة والتدابير المساءلة عبر الأنظمة القضائية المختلفة. تكشف النتائج عن وجود فجوة كبيرة بين الابتكار التكنولوجي

السريع وتطوير الضمانات القانونية الفعّالة، مما يُظهر أن العديد من أنظمة المراقبة لا تفي بمبادئ الشرعية والضرورة والتناسب التي تفرضها قوانين حقوق الإنسان.

وتؤكد النتائج أن المراقبة غير المقيدة وغير الشفافة تُهدد الحكم الديمقراطي، وتضعف الثقة العامة، وتخاطر بتطبيع انتهاكات الخصوصية. ويخلص البحث إلى أن الأمن الحقيقي لا يتحقق إلا من خلال مواءمة ممارسات المراقبة مع معايير حقوق الإنسان عبر تشريعات أقوى، ورقابة أخلاقية فعّالة، وتعاون عالمي، بما يضمن أن تكون التكنولوجيا وسيلة لتعزيز كرامة الإنسان وحريته لا تهديدًا لهما.

Abstract

The rapid advancement of digital surveillance technologies has transformed the relationship between state security and the protection of individual rights. With the widespread use of biometric identification, artificial intelligence, and large-scale data analytics, surveillance has become a central feature of modern governance while simultaneously raising profound legal, and human rights challenges. This study investigates how surveillance practices intersect with the principles of privacy, freedom, and accountability enshrined in international instruments such as the *Universal Declaration of Human Rights (UDHR)* and the *International Covenant on Civil and Political Rights (ICCPR)*.

Using a qualitative and doctrinal research approach, the paper analyzes international treaties, academic works, and policy frameworks to assess how states justify and regulate surveillance in the name of national security. It adopts a comparative lens to examine variations in legal standards, oversight mechanisms, and accountability measures across jurisdictions. The research reveals a significant gap between rapid technological innovation and the development of effective legal safeguards, showing that many surveillance systems fail to meet the principles of legality, necessity, and proportionality mandated by human rights law.

The findings highlight that unchecked and opaque surveillance threatens democratic governance, weakens public trust, and risks normalizing intrusions on privacy. The study concludes that true security requires aligning surveillance practices with human rights norms through stronger legal regulation, ethical oversight, and global cooperation, ensuring that technology enhances—rather than endangers—human dignity and freedom.

1-Introduction

Surveillance and tracking technologies—particularly digital surveillance technologies (DSTs)—have expanded dramatically over the past decades, becoming integral to

Journal of Babylon Center for Humanities Studies: 2026, Volume: 16, Issue: 1

both governmental and corporate systems of control, communication, and security. These technologies, ranging from closed-circuit television (CCTV) networks and facial recognition systems to artificial intelligence–driven data analytics, now form the backbone of many modern security infrastructures. As Fletcher (2023, p.30) observes, the proliferation of these systems has compelled governments worldwide to engage seriously with concerns surrounding privacy and related human rights. This expansion has transformed how states and institutions monitor individuals, raising fundamental questions about the balance between security imperatives and the protection of civil liberties.

Modern surveillance systems are characterized by their efficiency, reach, and automation. They are not only more cost-effective but, in certain respects, less reliant on intrusive human methods such as physical monitoring or direct observation. Governments increasingly depend on technology—rather than human spies or informants—to conduct surveillance. Common practices include the monitoring of public spaces via CCTV, the automated interception of internet and telecommunications data, and the deployment of artificial intelligence (AI) systems to analyze vast troves of information. As Lyon (2007, pp.45-47) and Königs (2022, p.2) explain, this shift toward automation has produced a paradox: while surveillance has become more pervasive, direct human interaction with collected data has declined. Consequently, some argue that this technological mediation may reduce privacy invasion, as most data is never directly viewed by human analysts. However, as AI capabilities advance, human oversight continues to diminish, intensifying the debate about whether such developments genuinely safeguard privacy or merely conceal new forms of control.

The digital age has thus created a landscape in which the boundaries between security and freedom are increasingly contested. As Nguyen and Tran (2023) note, societies are confronting an urgent dilemma: how to reconcile the demands of national and public security with the fundamental rights of individuals. The global expansion of data-driven governance—where governments and corporations collect, analyze, and distribute information on an unprecedented scale (Debbarma, 2023) has sparked profound concern about potential infringements on personal autonomy. Cotula (2020) emphasizes that surveillance technologies, if left unchecked, can undermine human rights by enabling disproportionate state power and eroding privacy protections. In this context, Nandy (2023, p.13) argues that understanding and redefining human rights amid this technological transformation is essential, requiring careful calibration between freedom and control.

States have become increasingly reliant on surveillance, artificial intelligence, and machine learning in governance, particularly in intelligence gathering and law enforcement (Makoni, 2022; Ryan-Mosley, 2022). Predictive policing systems, as described by Deeks (2018) and Oswald et al. (2018), exemplify how algorithmic decision-making reshapes state–citizen relationships by enabling the state to monitor behavioral patterns and identify potential risks. Similarly, the Court of Justice of the European Union (CJEU) has highlighted in the *Tele2 Sverige and Watson* (2016) cases that such data collection architectures can constitute a serious intrusion into private life, emphasizing the necessity for legal safeguards. Wyden et al. (2006, p.352) stress that balancing security and civil liberties is an ongoing process rather than a fixed goal; policymakers must treat both values as equal priorities, resisting fear-driven policies that threaten democratic foundations.

Technological advancement has revolutionized nearly every aspect of human life. As Mark (2024, p.433) observes, the digital revolution has yielded enormous social and economic benefits while simultaneously creating unprecedented ethical and legal challenges concerning privacy, justice, and freedom. Surveillance technologies, including biometrics, facial recognition, and online tracking, have intensified these debates by enabling real-time monitoring of individuals' movements, communications, and relationships. While these systems serve legitimate purposes such as crime prevention and national security, they also risk violating core human rights if implemented without sufficient oversight (Lynch, 2024). Cain (2023) highlights the global significance of this dilemma, noting that the challenge of balancing security needs with civil liberties transcends national boundaries and requires adaptable legal frameworks responsive to technological change.

The ethical implications of surveillance extend beyond mere privacy concerns. Bailey (2013, p.44) warns that AI-driven surveillance tools can reinforce social biases, disproportionately impacting marginalized communities. Similarly, Javvaji (2023, p.117) finds that facial recognition technologies frequently misidentify individuals from minority groups, raising questions of fairness, discrimination, and due process. The normalization of such pervasive surveillance can also exert a "chilling effect" on free speech and public assembly, as individuals modify behavior under constant observation (Javvaji, 2023, p.119). Addressing these challenges requires a comprehensive framework that prioritizes transparency, algorithmic accountability, and human oversight.

A nuanced understanding of surveillance, as Galič et al. (2017, p.10) explain, must account for its diverse forms—ranging from secret policing in authoritarian regimes to mundane workplace monitoring. The term *surveillance* itself, derived from *sur* ("from above") and *veillance* ("to watch"), encapsulates hierarchical power relations embedded in observation. Lyon and Zureik (1996, p.3) describe surveillance as the "monitoring of populations for specific purposes," while Lyon (1994, p.4) elaborates that participation in modern society inevitably entails a degree of electronic monitoring—whether through credit card use, border crossings, or digital communication. Importantly, Lyon (1994, p.5) emphasizes that surveillance is both "caring and controlling," simultaneously ensuring social order and facilitating welfare. Thus, modern surveillance is not inherently good or bad but rather a complex interplay between protection and control.

At its core, the discourse on surveillance and human rights revolves around a fundamental tension: security cannot exist without freedom, yet freedom becomes meaningless without security. Fletcher (2023, p.30) underscores that the challenge lies in developing governance frameworks capable of balancing these imperatives. This balance requires the active participation of policymakers, technologists, civil society, and the public in crafting transparent and equitable systems. As Akram et al. (2020) and Partow-Navid and Skusky (2023) argue, effective surveillance governance depends on clearly defined legal boundaries, independent oversight, and procedural safeguards to prevent abuse. Public confidence in such systems can only be maintained through openness, judicial review, and participatory decision-making processes.

In this context, international cooperation becomes crucial. As security threats increasingly transcend national borders, nations must collaborate on intelligence sharing and regulatory standards while maintaining respect for privacy and human

rights. Veerabhadraiah and Gayathri Bai (2024, p.77) observe that the digital transformation of governance and communication has reshaped how citizens engage with institutions, demanding new global norms for accountability and protection. Ultimately, as Daniel Solove (2010, p.95) notes, the justification that individuals should surrender privacy for security is deeply problematic; it oversimplifies the complex relationship between freedom, trust, and technology in democratic societies.

Thus, in an age of ubiquitous surveillance, the pursuit of security must not eclipse the preservation of liberty. The challenge for policymakers and societies alike is to navigate this evolving terrain with wisdom, restraint, and a steadfast commitment to human dignity. Balancing surveillance and human rights requires not only technological innovation but also moral clarity—recognizing that freedom, once compromised, is rarely regained.

This research is significant as it explores one of the digital age's most pressing dilemmas: balancing national security with the protection of fundamental human rights. As surveillance technologies like CCTV, biometrics, and AI-driven analytics become more integrated into governance and daily life, the risk of human rights violations—particularly regarding privacy, equality, and freedom of expression—grows. The study contributes to global and academic discussions on surveillance ethics, human dignity, and legal frameworks that ensure technological innovation supports, rather than undermines, democratic values. By analyzing international laws, case studies, and ethical frameworks, it provides insights for policymakers, technologists, and human rights advocates to develop proportionate, rights-based surveillance policies.

The main objectives are to analyze how modern surveillance technologies affect privacy, equality, and freedom of expression; examine their ethical, legal, and social implications in national security and law enforcement; evaluate international legal standards and case law governing surveillance and data collection; identify principles such as legality, necessity, and proportionality to balance security with individual freedoms; and propose recommendations for transparent, accountable, and human rights–compliant surveillance frameworks.

The rapid growth of surveillance technologies has enhanced national security and public safety but intensified concerns about privacy violations, discrimination, and abuse of power. Governments often justify extensive surveillance for counterterrorism, yet such practices frequently lack oversight and legal restraint, raising the question: how can societies maintain security without eroding fundamental human rights? The tension lies between technological advancement and human dignity—the need for protection versus the right to freedom. The lack of global consensus and enforceable standards for regulating digital surveillance threatens both democracy and individual autonomy.

This research uses a qualitative, doctrinal approach, analyzing legal, ethical, and theoretical frameworks related to surveillance and human rights. The methodology includes a literature and documentary review of scholarly works, UN reports, international treaties (e.g., UDHR, ICCPR), and court rulings (e.g., CJEU, ECtHR). It incorporates case studies such as the Snowden disclosures, Bridges v. South Wales Police, and U.S. surveillance under FISA to examine real-world implications. Comparative legal analysis assesses how jurisdictions like the U.S., EU, and Australia balance privacy and security. Finally, a normative evaluation applies principles of

legality, legitimacy, and proportionality to determine whether current surveillance laws and practices meet international human rights standards.

2-Balancing Privacy, Human Dignity, and National Security

There is a clear tension between the state's duty to respect the right to privacy and its obligation to protect national security. The right to privacy encompasses freedom from interference in one's private life and communications. However, to combat threats such as organized crime and terrorism, governments may need to conduct investigations that involve monitoring private affairs and communications to obtain information necessary for preventing crimes or holding perpetrators accountable. These investigations often rely on electronic surveillance and interception of communications. Some countries have enacted specific legislation to regulate such interception, while in others, the authority is granted through counter-terrorism laws (African Commission on Human and Peoples' Rights, 2015, pp.12-13).

The use of surveillance and communication interception is justified and necessary in circumstances where the state aims to combat organized crime, terrorism, or similar threats. Nevertheless, serious concerns have arisen about the potential for such investigations to excessively infringe on individual privacy. Governments may also abuse these powers to spy on political opponents, using the information to suppress or stifle legitimate democratic activity (United Nations General Assembly,2013; United Nations Human Rights Council, 2014, para.14).

Thus, while surveillance and interception are essential tools for protecting fundamental rights against threats such as terrorism and organized crime, these measures simultaneously pose a significant risk to the enjoyment of the same rights, particularly the right to privacy (African Commission on Human and Peoples' Rights, 2015, pp.12–13; United Nations Human Rights Council, 2014, para.14).

As Balule & Otlhogile (2015, pp.19–32) observe, surveillance can lead to the collection and storage of personal data and private information, which may be aggregated to create detailed profiles of targeted individuals, resulting in a significant invasion of privacy. In response, the international community has developed principles and guidelines to regulate communications surveillance. One of the core principles emphasized is proportionality, ensuring that surveillance measures are appropriate and not excessive relative to the intended objective (United Nations General Assembly, 2014, para.51; United Nations Human Rights Council, 2017, paras.30–39).

Where communication surveillance is necessary, it must be conducted in accordance with the law and in a proportionate manner. Guidelines and principles developed by experts are generally not legally binding, unless they have become part of customary international law or an international treaty ratified by states. This raises a challenge, as the principle of proportionality may be treated as a guideline rather than a binding rule, particularly when governments face serious national security threats. However, this argument holds less weight in jurisdictions bound by the ICCPR, because the Human Rights Committee has interpreted Article 17 to require that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case" (*Toonan v. Australia*, 1994, para.8.3; *Antonius Cornelis Van Hulst v. Netherlands*, 2000, para.7.3; *M.G. v. Germany*, 2007, paras.10.1–10.2).

The scope of privacy is deeply shaped by a society's political philosophy and system of governance. In authoritarian systems, where the state seeks to control individual

behavior, personal autonomy is limited, and the sphere of privacy is narrower. In contrast, liberal democracies value individual autonomy, allowing for a broader realm of privacy and stronger protection of personal freedoms (Westin, 2003, pp. 432–433).

However, privacy norms are not static—they evolve with societal values and intergenerational shifts. What one generation considers private may not hold the same meaning for another. As Allan Westin notes, debates over privacy are "never-ending" because they are tied to changing social norms about which types of conduct are considered beneficial or harmful to the public good (Westin, 2003, p. 433).

Despite its changing nature, the right to privacy remains fundamental, encompassing freedom from unlawful surveillance of one's person, relationships, or communications. Yet, this right often clashes with state efforts to protect national security, especially during crises. In many cases, governments emphasize granting wide surveillance powers while neglecting adequate safeguards to prevent disproportionate intrusions into privacy (Palmer, 2016).

The argument that privacy should yield to security is flawed, as it overlooks the purpose of privacy—to protect human dignity. As Floridi (2013) and Ackermann (2014) argue, dignity rests on the recognition of an individual's inherent worth, autonomy, and capacity to form independent judgments and relationships (Floridi, 2013, p. 308; Ackermann, 2014, pp. 23-24, 56). The UN Special Rapporteur on the Right to Privacy similarly emphasizes that privacy is integral to preserving dignity and autonomy.

Beyond personal dignity, privacy underpins the exercise of other fundamental rights. Without a protected private sphere, individuals cannot freely develop opinions, associate, or communicate without fear of state surveillance. The UN General Assembly Resolution 68/167 recognizes that privacy is essential for the enjoyment of freedom of expression, association, and political participation . Even socio-economic rights, such as the right to health, depend on privacy; without it, individuals may avoid seeking sensitive medical advice for fear of exposure.

Arguments that national security must override privacy—especially in states facing terrorism or instability—ignore the interdependence between the two. As seen in Egypt's Counterterrorism Law (2015), excessive surveillance powers can erode democratic foundations (Human Rights Watch, 2015). National security cannot be achieved by undermining the very freedoms it aims to protect. A society thrives only when individuals are free to develop, associate, and think independently.

Thus, privacy is not a luxury but a necessity—a prerequisite for human flourishing, democratic participation, and social stability. Governments must therefore ensure that surveillance laws strike a proportionate balance between protecting national security and upholding individual rights. The protection of privacy ultimately sustains both human dignity and national security.

In my view, the relationship between privacy and national security should not be seen as a zero-sum conflict but as a balancing act that defines the strength of a democracy. While national security is essential for protecting citizens, it should never be used as a blanket justification for violating privacy or restricting civil liberties. Too often, governments invoke "security" as a pretext for excessive surveillance or censorship, which undermines trust, accountability, and the very freedoms that security is meant to safeguard.

The principle of proportionality offers a sound legal and ethical framework for this balance — ensuring that state interference with privacy remains lawful, necessary,

and limited to the least intrusive means. When governments adhere to these principles, security measures can coexist with respect for human rights. However, when they are ignored, surveillance becomes a tool of control rather than protection.

I believe privacy is not merely a personal preference but a pillar of human dignity and autonomy, as scholars like Floridi (2013) and Ackermann (2014) emphasize. Without privacy, individuals lose the space to think, communicate, and dissent freely — all of which are essential for democratic participation. Therefore, protecting privacy is not contrary to national security; rather, it reinforces long-term security by preserving the legitimacy and moral authority of the state.

3-Security Benefits of Surveillance

The role of surveillance in crime prevention and national security has evolved significantly, driven by rapid technological advancements and the increasing sophistication of law enforcement tools. Modern surveillance systems, ranging from CCTV and digital monitoring tools to AI–powered analytics, have enhanced governments' and security agencies' capacities to deter criminal activities, respond to incidents effectively, and gather critical evidence for prosecution (Wheatley, 2024, p. 2). The adoption of these technologies reflects a broader shift toward data-driven policing and proactive security measures, where predictive analytics and real-time monitoring allow authorities to anticipate and mitigate threats before they escalate.

CCTV systems, for instance, have demonstrated considerable effectiveness in reducing crime, particularly in urban environments and public spaces. A meta-analysis conducted by Welsh and Farrington highlights that surveillance, especially in car parks and transport hubs, significantly reduces incidents of vehicle-related crimes, illustrating the direct impact of visible monitoring on criminal behavior (Wheatley, 2024, p. 2). Similarly, extensive CCTV coverage in city centers and high-risk neighborhoods has been associated with measurable declines in theft, vandalism, and other offenses. The presence of cameras acts as a deterrent, as potential offenders are acutely aware that their actions may be observed and recorded, thereby increasing the perceived risk of apprehension (Wheatley,2024, p. 2). This phenomenon aligns with the Hawthorne effect, where individuals modify their behavior simply because they know they are being watched (Wheatley,2024, p. 2).

Beyond deterrence, surveillance technologies enhance operational efficiency by enabling rapid law enforcement responses. Integrated monitoring systems, where CCTV feeds are linked to centralized control rooms, allow authorities to allocate resources strategically, respond to incidents in real time, and minimize the impact of criminal activity. For example, high-risk areas can be continuously monitored, and alerts triggered automatically when suspicious behavior or unusual patterns are detected. Such responsiveness not only prevents crimes from escalating but also facilitates early intervention in emergency situations, such as armed robberies, assaults, or public disturbances (Wheatley, 2024, p. 2).

Digital surveillance, augmented by AI and machine learning, further refines crime prevention strategies. Advanced algorithms can analyze vast amounts of video and sensor data to identify patterns of behavior, flag anomalies, and even predict potential criminal activity (Wheatley, 2024, p. 2). Facial recognition technologies, for example, can assist authorities in identifying suspects on watchlists in crowded public spaces or at transportation hubs, thereby preventing potential criminal incidents before they occur. Machine learning models can also reduce human error and bias in decision-

making, enhancing the accuracy of threat detection while ensuring a more consistent application of security measures (Wheatley, 2024, p. 2).

Surveillance technologies play a similarly crucial role in national security, particularly in counterterrorism operations, where early detection and disruption of threats are imperative. Governments employ a variety of tools, including high-resolution cameras, biometric scanners, and advanced data analytics, to monitor individuals, organizations, and communications for indicators of extremist activity (Wheatley, 2024, p. 3). The integration of these systems allows security agencies to identify and track individuals who may pose a threat, intervene at critical moments, and prevent attacks on public spaces, transportation networks, and critical infrastructure. Networked CCTV systems combined with facial recognition, for example, have enabled law enforcement to monitor high-traffic areas, detect persons of interest, and coordinate responses across multiple jurisdictions, enhancing both preventive and reactive security measures (Wheatley,2024, p.3).

Monitoring digital communications—including emails, phone calls, social media posts, and other forms of online interaction—also forms an essential component of modern counterterrorism surveillance. By analyzing communication patterns and online behavior, authorities can identify potential threats, disrupt terrorist networks, and prevent the coordination of criminal or extremist activities (Wheatley, 2024, p.3). In addition, surveillance extends to cyberspace, where sophisticated tools detect cyber threats targeting state infrastructure, financial systems, and critical services. Cyber surveillance protects national assets such as power grids, government databases, and communication networks, all of which are increasingly vulnerable in modern conflicts and hybrid warfare scenarios (Wheatley,2024, p.3).

Satellite imagery and electronic signals intelligence further enhance national security by providing oversight of military activities, border security, and compliance with international agreements. For instance, satellite monitoring can reveal unauthorized military developments or troop movements that could indicate emerging threats, allowing states to respond proactively and maintain strategic stability (Wheatley,2024,p.3). Combined with terrestrial and digital surveillance, these technologies provide a comprehensive framework for protecting national interests while mitigating risks to public safety.

Despite these clear security benefits, the expansion of surveillance technologies raises important ethical and legal questions. The collection of data on individuals, even for legitimate security purposes, poses potential threats to civil liberties, including privacy, freedom of expression, and protection from arbitrary state action (Javvaji, 2023, p.179). Oversight mechanisms, clear legal boundaries, and transparent governance structures are therefore critical to ensure that surveillance measures remain proportionate, accountable, and consistent with democratic principles. Without such safeguards, there is a risk that the same technologies designed to protect citizens could be misused, undermining trust in government institutions and eroding public confidence in security frameworks (Javvaji, 2023, p. 179).

Surveillance also plays a key role in forensic investigations, providing essential visual and digital evidence that supports legal proceedings. High-resolution footage from CCTV cameras, body-worn devices, and drones can document events, reconstruct crime scenes, and identify suspects, thereby strengthening the judicial process (Javvaji, 2023, p.179). Such evidence not only facilitates prosecutions but also contributes to broader public accountability, demonstrating that security agencies

operate within established legal and ethical frameworks. The ability to collect and analyze forensic data efficiently enhances investigative accuracy and ensures that justice is served while minimizing wrongful convictions or procedural errors.

Moreover, surveillance systems are indispensable for safeguarding critical infrastructure, including airports, seaports, transportation hubs, government buildings, power plants, and healthcare facilities. These sites are often high-value targets for terrorism, sabotage, or organized crime. Intelligent monitoring systems, equipped with intrusion detection, access control, and perimeter security measures, allow authorities to prevent unauthorized access, identify threats, and coordinate rapid responses in case of breaches (Javvaji, 2023, p.179). By integrating these systems with broader security networks, organizations can maintain continuous oversight of sensitive areas, enhancing both physical and operational security.

The cumulative effect of these capabilities is a measurable enhancement of societal security and public safety. By deterring criminal acts, enabling rapid response to incidents, and providing reliable forensic evidence, surveillance technologies contribute to safer communities and foster public confidence in law enforcement and security institutions (Wheatley,2024, p. 2; Javvaji, 2023, p. 179). At the national level, they bolster resilience against a wide spectrum of threats, from ordinary criminal activity to terrorism, cyberattacks, and international conflicts. While debates over ethical and privacy concerns persist, empirical evidence consistently demonstrates that well-designed surveillance frameworks play a critical role in maintaining order, protecting citizens, and supporting the rule of law.

The security benefits of surveillance are multifaceted, encompassing crime prevention, real-time monitoring, forensic support, national security, and the protection of critical infrastructure. Technologies such as CCTV, AI-driven analytics, facial recognition, and cyber surveillance enhance law enforcement and counterterrorism capabilities while promoting public safety and operational efficiency (Wheatley, 2024, pp. 2-3; Javvaji, 2023, p.179). However, these benefits must be balanced against the potential risks to civil liberties, privacy, and democratic governance. Implementing robust oversight, legal safeguards, and transparent operational policies ensures that surveillance technologies achieve their security objectives while respecting fundamental human rights.

In my view, surveillance plays a crucial role in public safety and national security. Technologies like CCTV, AI analytics, and facial recognition enhance crime prevention, rapid law enforcement response, and forensic investigations, allowing authorities to act proactively and protect critical infrastructure against complex threats. However, these benefits come with significant ethical and legal risks. Without clear oversight, transparency, and safeguards, surveillance can intrude on privacy, enable profiling, and undermine public trust. Overall, surveillance is a double-edged sword: highly effective for security but requiring careful regulation. When responsibly designed and monitored, it can protect citizens while upholding fundamental human rights and democratic principles.

4- Human Rights and Technology in National Security

The intersection of emerging technologies and national security has become a key focus of human rights scholarship and international governance. New systems—ranging from AI and big data analytics to biometric surveillance and predictive policing—are transforming how states identify threats, manage borders, and conduct intelligence operations. While these technologies promise enhanced efficiency and

Journal of Babylon Center for Humanities Studies: 2026, Volume: 16, Issue: 1

security, they simultaneously raise major ethical, legal, and human rights concerns related to privacy, discrimination, and accountability.

Predictive policing technologies, used in countries such as the United States and the United Kingdom, illustrate how AI-driven systems can both strengthen and endanger human rights. By analyzing crime data to forecast where offenses are likely to occur, these systems aim to improve law enforcement efficiency. However, research shows that predictive models often reproduce racial and socioeconomic biases found in historical data, leading to disproportionate targeting of minority communities (Lum and Isaac, 2016, p.17). In cities like Los Angeles and Chicago, predictive policing initiatives were criticized for reinforcing discriminatory surveillance rather than reducing crime (Ferguson, 2017, p.103). These cases highlight the need for algorithmic transparency and human oversight to prevent technology from amplifying inequality.

Facial recognition technology (FRT) has become a core tool in national security efforts, particularly in border control, law enforcement, and counterterrorism. China's extensive use of FRT in public spaces—especially in the Xinjiang region—has been condemned for violating privacy, freedom of movement, and equality rights (Human Rights Watch, 2019, p.5). Similarly, in Western democracies, the use of facial recognition by the United Kingdom's Metropolitan Police has raised concerns over consent and proportionality (Smith & Mann, 2017, pp. 122-123). The *Bridges v. South Wales Police* (2020) ruling established that indiscriminate use of FRT breaches privacy and equality laws, demonstrating that while these systems can support public safety, they risk undermining civil liberties when left unregulated.

Biometric identification systems—such as fingerprint, iris, and voice recognition—are increasingly employed in national security programs and humanitarian contexts. The United Nations High Commissioner for Refugees uses biometric registration to streamline aid delivery, yet the storage and exchange of such sensitive data introduce risks of misuse, breaches, and surveillance. In India, the Aadhaar biometric system, designed to enhance welfare access, sparked significant privacy concerns and led to the 2017 Supreme Court ruling that recognized privacy as a fundamental right. These cases expose the tension between efficiency, data governance, and the protection of individual rights within global security and welfare systems.

Since 9/11, governments have expanded mass data collection to combat terrorism and cyber threats. The U.S. National Security Agency's surveillance programs—revealed by Edward Snowden in 2013—exposed widespread monitoring of citizens' communications without sufficient judicial oversight, challenging compliance with Article 17 of the International Covenant on Civil and Political Rights (Greenwald, 2014, p.56). In Europe, similar controversies led to landmark rulings by the Court of Justice of the European Union (*La Quadrature du Net and Others v. France, 2020; Tele2 Sverige AB v. Watson and Others, 2016)*) restricting indiscriminate data retention. These developments underline the enduring conflict between state security imperatives and the right to privacy in the digital age.

These issues are mirrored in real-world cases. The *Harun Causevic* case in Australia demonstrates the extension of counter-terrorism powers through electronic surveillance and control orders imposed without sufficient evidence, raising serious concerns over freedom of movement, privacy, and expression under Articles 12, 17, and 19 of the ICCPR (Bonnefont, 2024, p.4). Similarly, *U.S. v. Muhtorov* shows how Section 702 of the Foreign Intelligence Surveillance Act (FISA) enables warrantless

data collection later used in criminal proceedings, undermining due process and fair trial rights (Bonnefont, 2024, p.5). In *Al-Haramain Islamic Foundation v. U.S. Treasury*, the invocation of the state-secrets privilege blocked challenges to unlawful surveillance and asset freezes, revealing how secrecy can hinder judicial oversight and access to remedies (Bonnefont, 2024,p. 6).

Bonnefont (2024,pp. 6-11) also highlights the *ZeroFOX* case, where a private contractor conducted social media monitoring of political activists under government contract. These activities, insulated from Freedom of Information Act obligations, created chilling effects on free speech and assembly. Likewise, European Court of Human Rights cases such as *Weber and Saravia v. Germany* and *Szabó and Vissy v. Hungary* emphasize that mass or indiscriminate surveillance—including through drones—must have clear legal safeguards and judicial authorization. The Snowden revelations further exposed the scale of bulk metadata collection, sparking limited reforms but leaving unresolved concerns about profiling and cross-border data exchange.

Bonnefont (2024, pp.12-15) also examines biometric surveillance in security and humanitarian operations. Systems such as Australia's National Facial Biometric Matching Capability, the U.S. military's SEEK database, and the UN's iris-scanning programs for refugees raise concerns about consent, data protection, and discrimination, especially when biometric registration becomes mandatory for accessing aid or movement. Moreover, algorithmic bias in facial-recognition and emotion-analysis technologies systematically misclassifies women and minorities, resulting in discriminatory policing outcomes and violations of equality before the law.

Taken together, these case studies reveal a consistent pattern: the rapid expansion of surveillance and data-driven technologies has outpaced the development of adequate human rights safeguards. Across contexts—from counter-terrorism to humanitarian governance—Bonnefont identifies opacity, weak oversight, and blurred boundaries between state and private actors as core causes of rights violations . While national security frameworks justify these technologies as necessary for rapid threat detection, the cumulative effect has been a gradual normalization of exceptional powers and invasive data practices that erode privacy, due process, and equality.

Comparatively, both Australia and the United States exhibit broad discretionary powers and limited judicial scrutiny, whereas European systems apply stronger proportionality tests. Still, emerging tools like autonomous drones and predictive analytics increasingly challenge even robust legal standards. Bonnefont (2024, pp.14-21) concludes that reconciling technological innovation with human rights obligations requires transparent statutory limits, independent oversight, and algorithmic impact assessments to prevent discrimination and ensure accountability.

Ultimately, the relationship between human rights and national security technologies is one of conditional complementarity: security and liberty can reinforce each other only within frameworks grounded in accountability, proportionality, and respect for human dignity.

Emerging surveillance technologies are powerful tools for national security, but they pose serious risks to privacy, equality, and civil liberties. I believe strong oversight, transparency, and human-rights–centered regulation are essential to ensure security does not come at the expense of individual freedoms.

Journal of Babylon Center for Humanities Studies: 2026, Volume: 16, Issue: 1

5- Surveillance and Human Rights

Surveillance impacts the enjoyment of various human rights, both positively and negatively. On one hand, it can support rights such as the right to life and certain social and economic rights. For instance, government collection of health data may improve disease prevention, personalized treatment, and public health planning—helping the state fulfil its human rights obligations.

However, surveillance also raises serious human rights concerns, particularly regarding privacy and non-discrimination. While some may view surveillance as necessary for safety and social progress, it can easily become intrusive, undermining individual freedoms and equality. The following sections explore how surveillance interacts with these core human rights.

5-1 Surveillance and the Right to Privacy

The most direct and immediate human right affected by surveillance is the right to privacy. As Alan Westin defines it, privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7). This definition underscores privacy as a fundamental dimension of human autonomy, enabling individuals to control information about themselves and maintain personal boundaries. Privacy is not merely a theoretical concept; it is foundational within the international human rights framework and recognized universally across international, regional, and national legislations. The Office of the High Commissioner for Human Rights (OHCHR) emphasizes the universal importance of privacy, highlighting the necessity for both legal protections and practical safeguards to ensure that personal freedoms are preserved (OHCHR, 2014, para. 11).

The recognition of privacy as a human right is entrenched in major international instruments. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) explicitly guarantee the right to privacy, protecting individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence, as well as attacks on their honor and reputation (UNGA, 1948; UNGA, 1966). The Human Rights Committee (HRC), in its interpretation of Article 17, clarifies that "arbitrary" interference refers not only to illegal acts but also to lawful interventions that are unreasonable, unnecessary, or inconsistent with the provisions of the Covenant (UNHRC, 1988, para. 4). Furthermore, Article 17(2) of the ICCPR ensures that individuals have legal remedies to protect themselves against such violations, highlighting the proactive responsibilities of states in safeguarding privacy (ICCPR, 1966).

Under international human rights law, states have three complementary obligations with regard to human rights: to respect, protect, and fulfill them (de Schutter, 2014, p. 280). Respecting privacy requires that states refrain from unlawful interference in personal affairs, ensuring that citizens' dignity and autonomy are not compromised. Protection extends to preventing third-party violations, including those perpetrated by private corporations or organizations, and fulfilling the right demands that adequate legal frameworks be established to prevent violations while providing effective remedies for victims (UNHRC, 2014). In the context of surveillance, these obligations translate into the necessity for states to ensure that monitoring activities—whether conducted by public authorities or private actors—are strictly necessary, lawful, and proportionate to the objectives pursued.

However, the right to privacy is not absolute. As de Schutter notes, human rights generally operate within a framework of relative limitations that permit lawful interference under certain conditions (de Schutter, 2014, p. 339). These limitations are typically evaluated against three fundamental criteria: legality, legitimacy, and proportionality. The legality criterion mandates that any restriction on privacy must be clearly prescribed by law, publicly accessible, and aligned with international human rights standards. This principle finds support in Article 4 of the ICCPR, which outlines the permissible derogations from certain rights during times of emergency. Since Article 17 of the ICCPR is not a non-derogable right, states may impose restrictions under specified conditions (ICCPR, Article 4).

The legitimacy criterion requires that surveillance measures serve lawful purposes such as national security, public safety, or public health. Surveillance laws must be precise, specifying who may be monitored, under what circumstances, and for what duration (OHCHR, 2014, p.28). Proportionality ensures that the intrusion into privacy is no greater than necessary to achieve the legitimate objective, compelling governments to establish robust safeguards, minimize data collection, and provide remedies for individuals adversely affected by surveillance (UNHRC, 2014).

When evaluating the right to privacy in the context of modern surveillance, it is useful to consider three axes: the actors involved, the mode of surveillance, and the scope of impact. While human rights law primarily regulates the relationship between states and individuals, it also obliges states to protect citizens against violations by third parties, including corporations and other non-state actors. The impact of surveillance varies according to type: for example, public CCTV systems affect large populations in a relatively superficial manner, whereas targeted covert monitoring of individuals may result in deeper and more intrusive privacy violations (Galič, Timan, & Koops, 2017, p. 30).

The legal framework protecting privacy is extensive, spanning international, regional, and national instruments (ICCPR, Article 17). Yet, the rapid development of surveillance technologies often outpaces legal safeguards, creating gaps that challenge traditional notions of privacy. The rise of digital consent mechanisms, such as agreeing to terms of service or data collection policies on social media and mobile applications, blurs the line between voluntary information sharing and intrusive surveillance (Matzner, 2018, p. 73; Nemitz, 2018, p. 9). Modern surveillance inherently involves collecting personal information, from visible monitoring through CCTV to covert practices like email or mobile tracking, which constrains autonomy and narrows the practical scope of privacy. States bear the responsibility to regulate private surveillance, but this obligation becomes complex when individuals voluntarily disclose personal information online, creating ambiguity regarding consent and data ownership.

Privacy is intrinsically linked to other human rights, often serving as a “gatekeeper” for freedoms such as expression, association, and dignity (McGregor et al., 2018, p. 8). Surveillance, particularly in the digital era, heightens the potential for discrimination, social control, and inequality, all of which undermine democratic freedoms. The balance between national security and privacy is delicate: while security is a legitimate concern, excessive surveillance risks eroding civil liberties and fostering a climate of mistrust (Chadha, 2022). Surveillance technologies, such as facial recognition, online tracking, and mobile monitoring, have the potential to enhance security efforts but simultaneously threaten personal privacy (Kumar, 2023;

Nandy, 2023). Smartphones, for instance, can act as "24-hour surveillance devices," capturing sensitive information about location, communication, and behavior (United Nations, 2022).

International legal instruments have consistently affirmed privacy as a fundamental right. UDHR Article 12 recognizes the protection of privacy, family, home, correspondence, honor, and reputation, while ICCPR Article 17 reiterates similar protections with explicit emphasis on unlawful interference (Diggelmann & Cleis, 2014, pp. 447–449). Moreover, the UN Guidelines Concerning Computerized Personal Data Files (E/CN.4/1990/72) and OECD Guidelines on transborder data flows (Paris, 1980) address privacy in the context of electronic data, highlighting the need for oversight in the digital domain. The Human Rights Committee, through General Comment No. 16, further clarified that privacy encompasses protection against interception of communications, wiretapping, and electronic monitoring, emphasizing that national laws must safeguard these rights (OHCHR, 1988, p. 8).

Despite comprehensive legal frameworks, implementation gaps persist. Blanket or covert surveillance, mass data collection, and pervasive monitoring undermine autonomy and public expectations of privacy, raising pressing ethical concerns. The UN Special Rapporteur in 2013 stressed that privacy constitutes a "private sphere" essential for autonomous development and freedom from excessive state or third-party interference (La Rue, 2013, p. 17). Furthermore, secure and private communications, including the ability to remain anonymous online, are vital for exercising freedom of expression and participation in society without fear of retribution (La Rue, 2013, pp. 6-11).

The intersection of surveillance and the right to privacy presents a profound challenge in the contemporary era. While international law provides detailed frameworks for protecting privacy, technological advances have outpaced legal adaptation, creating vulnerabilities to both state and corporate overreach. The principles of legality, legitimacy, and proportionality, though foundational, are frequently undermined by opaque surveillance programs and broad national security claims. The role of private corporations—collecting, storing, and monetizing personal data—extends surveillance beyond state mechanisms, creating complex governance challenges largely unaccounted for in human rights law.

Consent in digital spaces has become increasingly problematic. Individuals rarely possess full knowledge of the scope, scale, and implications of surveillance embedded in platforms, rendering the distinction between voluntary data sharing and coercive observation tenuous. Privacy should therefore be conceptualized not only as an individual right but as a collective social good, essential for personal autonomy, democratic participation, and the protection of interconnected human rights. Balancing national security and surveillance with robust privacy protections remains one of the most pressing challenges of the 21st century, requiring transparency, accountability, technological literacy, and adaptive legal frameworks (Nandy, 2023; Kumar, 2023; Chadha, 2022).

5-2 Surveillance and non-discrimination

The rights to non-discrimination and equality are foundational principles in international human rights law, explicitly affirmed in multiple treaties and declarations. These include Article 7 of the Universal Declaration of Human Rights (UDHR) and Articles 2 and 26 of the International Covenant on Civil and Political Rights (ICCPR), which guarantee equality before the law and protection from

discrimination (UNGA, 1948; UNGA, 1966). Non-discrimination is also embedded throughout numerous other international conventions, often linked to the enjoyment of specific rights. For example, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) make explicit reference to equality and the prohibition of discrimination as essential components in realizing all other rights (CEDAW, 1979; ICESCR, Article 2).

Many legal scholars and jurists argue that the right to equality before the law has attained the status of customary international law, meaning it binds all states regardless of treaty ratification (Vice-President Ammoun, 1971, p.64). Although the ICCPR does not contain a single, codified definition of discrimination, the Human Rights Committee (HRC) provides a comprehensive interpretation in its General Comment No. 18, describing discrimination as:

"Any distinction, exclusion, restriction or preference which is based on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms"

The Committee also clarifies that differential treatment does not necessarily constitute discrimination if it is based on reasonable and objective criteria and serves a legitimate aim consistent with the Covenant (UNHRC, 1989, para13).

Under international human rights law, states have a tripartite obligation to respect, protect, and fulfil the rights to equality and non-discrimination (De Schutter, 2014, pp. 647, 701). To respect these rights, states must refrain from enacting laws, policies, or enforcement practices that are discriminatory. In order to protect them, states are required to ensure that third parties, such as corporations or other private actors, do not engage in discriminatory conduct. Finally, to fulfil these rights, states must take proactive measures to promote equality, including implementing legislation and programs that address structural discrimination and guaranteeing access to remedies for victims.

However, the rights to equality and non-discrimination, like many others, are not absolute. According to de Schutter, limitations on these rights must satisfy the criteria of legality, legitimacy, and proportionality (De Schutter, 2014, p.339). While Article 4 of the ICCPR does not list Articles 2 or 26 as non-derogable, any restriction on equality must be lawful, pursue a legitimate purpose, and be proportionate to that purpose (ICCPR, Article 4).

This principle extends to surveillance practices, which may have discriminatory effects. Surveillance that differentiates based on race, ethnicity, religion, or other protected characteristics violates the principle of non-discrimination unless it meets the strict standards of legality and legitimacy. Thus, potentially discriminatory surveillance measures—such as profiling or targeted monitoring—must be precisely regulated, ensuring that law enforcement agencies do not apply policies arbitrarily (Gauthier v. Canada, 1999, p.14).

A landmark case illustrating these principles is R v. Immigration Officer at Prague Airport (2004), where the UK House of Lords ruled that British immigration officers systematically discriminated against Roma travelers. The court found that Roma individuals were routinely subjected to additional questioning "simply because they were Roma," and that such practices were inherently incompatible with both domestic

and international law (De Schutter, 2014, p.665). The court emphasized that even if the intention was national security or immigration control, the effect amounted to unlawful ethnic profiling, violating the essence of equality before the law.

From a legal and ethical standpoint, proportionality is central to assessing discriminatory surveillance. Even when surveillance pursues legitimate objectives such as national security, any discriminatory aspect must be narrowly tailored and accompanied by safeguards to prevent abuse and ensure accountability. Surveillance that disproportionately targets marginalized groups not only erodes public trust but also entrenches systemic inequality.

Surveillance can infringe upon the right to non-discrimination in multiple ways. First, at the data collection stage, surveillance mechanisms may intentionally or unintentionally focus on specific groups, leading to disproportionate monitoring and potential marginalization. Second, at the data analysis stage, both algorithmic and human biases can influence how collected information is interpreted and applied, further perpetuating discriminatory outcomes. Together, these stages demonstrate how surveillance practices can systematically undermine the principle of equality.

As illustrated in the Prague Airport case, surveillance can be directly discriminatory when it systematically targets individuals based on ethnicity or other identifiers. Conversely, modern surveillance technologies such as big data systems and AI algorithms may appear neutral by collecting information from all individuals equally. However, such systems are not free from bias. Algorithmic surveillance can perpetuate discrimination through biased datasets and spurious correlations that falsely link certain characteristics to criminality or risk (Matzner, 2018, p.72; Sætnan, 2018, p.23). Big data, though often perceived as objective, is shaped by human decisions about what data to collect and how to interpret it.

When analyzing surveillance through the three axes of surveillance—actors, methods, and scope—questions of equality and discrimination become central. The nature and intent of the institution conducting surveillance determine its legitimacy. For instance, collecting data to improve medical care is distinct from using surveillance to profile ethnic minorities; both involve observation, but the underlying purpose and potential for discrimination differ significantly. Furthermore, the power imbalance between those conducting surveillance (states or corporations) and those being monitored reinforces the potential for abuse.

The mode of surveillance also influences its discriminatory impact. Overt surveillance, such as visible CCTV in public areas, generally affects everyone within range and is less likely to discriminate. In contrast, covert surveillance, particularly when directed at specific groups without their knowledge, risks violating equality by denying individuals the opportunity to consent or challenge the intrusion. Collecting data from some individuals and not others undermines equality before the law, especially if such data influences judicial or administrative outcomes (De Schutter, 2014, p.665).

While widespread surveillance may seem non-discriminatory by encompassing entire populations, the selection and analysis of data can reintroduce bias. Even mass surveillance can reproduce inequalities if algorithms disproportionately flag or categorize certain groups as “risky.” Thus, the discriminatory potential of surveillance

lies not only in whom it targets but also in how the collected information is processed and acted upon.

The intersection of surveillance, equality, and non-discrimination presents one of the most complex ethical challenges of the digital era. Surveillance technologies, often justified under the guise of security and efficiency, risk reinforcing social hierarchies and marginalization. While international human rights law provides a robust framework against discrimination, the technological dimension of modern surveillance blurs traditional legal boundaries.

Algorithmic profiling and predictive policing, for example, can reproduce systemic biases hidden within datasets, transforming structural discrimination into automated injustice. The illusion of technological neutrality masks the ways data-driven systems can perpetuate inequality—discriminating not through overt prejudice but through patterns of correlation and categorization.

Moreover, covert surveillance erodes transparency and accountability, allowing discriminatory practices to persist under secrecy. The human rights principle of equality demands that states and corporations audit their surveillance systems, ensure algorithmic fairness, and uphold procedural safeguards for those affected.

Ultimately, the right to non-discrimination is not merely about equal treatment but about ensuring substantive equality—addressing both the intent and the impact of surveillance. Without rigorous oversight, even well-intentioned surveillance systems can reproduce social biases, compromising the very principles of justice and fairness that human rights law seeks to protect.

Surveillance can enhance safety and public services, but it poses serious risks to privacy, equality, and non-discrimination. I believe strong oversight, transparency, and safeguards are essential to ensure that surveillance protects society without reinforcing bias or undermining fundamental human rights.

6-Freedom of Information vs National Security

The balance between freedom of information and national security is a central issue in contemporary governance, particularly in contexts involving technological surveillance and public accountability. Freedom of information is a core democratic principle that enables citizens, journalists, and organizations to access information, hold governments accountable, and participate meaningfully in public life. It supports transparency, public trust, and the protection of other human rights. National security, conversely, prioritizes the protection of the state and its citizens from threats such as terrorism, espionage, cyberattacks, or internal unrest. While national security is undoubtedly a legitimate concern, it can come into conflict with freedom of information when authorities cite security risks to withhold information or limit public debate (La Rue, 2013, para. 20).

Historical and contemporary case law illustrates these tensions. For instance, in Peck v. United Kingdom (36 EHRR 41, 28 Jan 2003), the European Court of Human Rights (ECtHR) considered the difference between ordinary surveillance in public life and serious intrusions into private life, highlighting that monitoring must be proportionate and respect individual privacy (Toulson, 2007, p. 149). Similarly, in Malone v. Metropolitan Police Commissioner, the ECtHR reaffirmed that human rights obligations must prevail over national security justifications. In R (B. Mohamed) v. Secretary of State for Foreign and Commonwealth Affairs (Administrative Court, CO/4241/2008), the UK Divisional Court ordered disclosure

of documents concerning alleged torture, despite U.S. claims that revealing the information could compromise intelligence relations.

Freedom of information is closely tied to the broader right to freedom of expression, protected under Article 19 of the ICCPR and Article 19 UDHR. Article 19 ICCPR provides that everyone has the right to seek, receive, and impart information without interference, but it allows limitations in cases involving hate speech, incitement to violence, or threats to national security (UN Human Rights Committee, 1983, para. 2; Toulson, 2007, p. 149; General Comment No. 34, 2011, paras. 52–54). Limitations must satisfy the three-part test of legality, legitimate purpose, and necessity/proportionality (Kaye, 2015, para. 38).

In the digital age, anonymity and encryption have become essential safeguards for freedom of expression, privacy, and political participation. Courts in Canada, South Korea, the U.S., and under the ECHR have upheld anonymous expression, whereas countries like Brazil, Venezuela, Iran, Ecuador, and Russia impose identification requirements, limiting anonymity and potentially weakening online security (R. v. Spencer, 2014; Kaye, 2015, para. 38). States are encouraged to adopt less intrusive approaches than blanket restrictions, balancing privacy and free expression against legitimate national security concerns.

Technological surveillance—particularly digital and AI-driven systems—has become a routine aspect of national security strategies. AI can identify individuals with criminal records or detect suspicious behavior, contributing to preventive measures (Suman, 2023). Biometric methods such as facial recognition and fingerprinting are increasingly used, signaling a shift toward more invasive monitoring practices (Savov, 2016). While these measures enhance the state's ability to protect citizens, they pose significant risks to privacy, civil liberties, and human dignity (Lindau, 2022; Bernot, 2022). "Function creep," or the expansion of surveillance tools beyond their original purpose, exacerbates these concerns, blurring the boundary between legitimate security measures and potential authoritarian control (Tzanou, 2010).

The rise of the "surveillance society" demonstrates the tension between security and liberty. Governments increasingly rely on technological tools to monitor public spaces, as seen in widespread CCTV deployment in the UK. Proponents argue these systems enhance public safety and deter crime, while critics emphasize the potential for misuse and the erosion of privacy (Tzanou, 2010). This reflects a broader challenge: national security laws are typically designed to protect state interests, often at the expense of individual rights (Cameron, 2001, pp. 40–49). Article 19(3)(b) of the ICCPR clarifies that the exercise of freedom of expression may be restricted for national security, provided the limitations are lawful, necessary, and proportionate (Cameron, 2001, p. 49; Doswald-Beck, 2011, p. 415).

Cybersecurity introduces additional complexity. National cyber security is fluid, encompassing political, economic, social, and military dimensions, yet lacking universally agreed definitions or metrics for effectiveness (Wamala, 2011, pp. 42–43; K. Ziolkowski, 2013, p. 21). Strategies in the UK (2011), U.S. Department of Defense (2015), and Russia (2014) emphasize protection of information and communication systems vital to national stability but provide limited operational clarity. This ambiguity allows for broad discretionary application of cyber surveillance, raising concerns about proportionality and accountability.

Surveillance technologies can also produce chilling effects on freedom of expression. Individuals aware of monitoring may self-censor, avoid political participation, or

disengage from civil society (Murray et al., 2023). AI and machine learning amplify these risks by detecting dissenting opinions or minority voices, potentially deterring free expression (Brandon, 2023). Legal and ethical frameworks, therefore, must evolve alongside technology to ensure that surveillance does not undermine democratic participation, privacy, or human rights.

Historically, the recognition of freedom of information and expression dates back to the 1946 UN General Assembly Resolution 59(I), supported by states such as the U.S., UK, and France (P. Malanczuk, 2011, para. 5). Articles 19 UDHR and 19(2) ICCPR articulate the right to seek, receive, and impart information regardless of frontiers, forming the foundation of modern transparency regimes. UN General Comment No. 34 further affirms protection of all forms of expression—including spoken, written, artistic, and digital communications (United Nations Human Rights Committee,2011,para. 11). In 2013, UN Special Rapporteur Frank La Rue explicitly extended these protections to the Internet, emphasizing that technological advances must not limit fundamental rights (La Rue, 2013, p. 23; Human Rights Council, 2011).

The tension between freedom of information and national security is inherently complex, particularly in the context of modern surveillance technologies. While governments require tools to detect and prevent threats, excessive or poorly regulated surveillance risks undermining the democratic principles it is intended to protect. Surveillance technologies, especially AI-driven systems, can restrict free expression, erode trust, and create chilling effects on political participation (Murray et al., 2023; Brandon, 2023).

Balancing these competing interests requires adherence to international human rights law, emphasizing legality, necessity, and proportionality. States must ensure that limitations on information access are narrowly tailored, justified, and transparent. Moreover, cyber and digital security strategies should be revisited regularly to align with evolving threats while respecting individual rights (Wamala, 2011; Savov, 2016). Ultimately, effective governance demands not only the protection of state security but also robust safeguards for civil liberties, privacy, and the right to access information.

While national security is essential, it must not come at the expense of freedom of information and expression. I believe surveillance should be carefully regulated to ensure transparency, accountability, and respect for civil liberties, preventing chilling effects on public participation and democratic oversight.

Conclusion

The expansion of surveillance technologies in the digital era has profoundly reshaped the relationship between state power, individual rights, and democratic accountability. While innovations such as CCTV, biometrics, facial recognition, and artificial intelligence enhance public safety, national defense, and law enforcement efficiency, they also pose serious challenges to fundamental human rights—particularly privacy, equality, and freedom of expression. This study finds that the growing integration of surveillance into governance has outpaced the development of corresponding legal and ethical safeguards, leading to significant risks of abuse, discrimination, and erosion of public trust.

International human rights frameworks, including the *Universal Declaration of Human Rights (UDHR)* and the *International Covenant on Civil and Political Rights (ICCPR)*, provide a solid foundation for protecting privacy and equality. However,

many states invoke national security as a justification for extensive surveillance without adhering to the principles of legality, necessity, and proportionality. As demonstrated through case studies such as *Bridges v. South Wales Police*, *U.S. v. Muhtorov*, and *Tele2 Sverige AB v. Watson*, unchecked surveillance undermines democratic governance and human dignity. The right to privacy, far from being a personal preference, is a precondition for autonomy, freedom of thought, and meaningful participation in society. Similarly, algorithmic bias and discriminatory profiling reveal that surveillance can entrench inequality when not subject to oversight and accountability.

Ultimately, the research concludes that security and freedom are not opposing goals but interdependent values. True national security must rest upon respect for human rights and the rule of law. The challenge for modern societies lies in creating governance systems that harness technological innovation while preserving civil liberties. Balancing surveillance and human rights demands a holistic approach—combining legal reform, ethical reflection, and international cooperation—to ensure that digital progress strengthens rather than weakens democracy.

Recommendations

1.Align national laws with international human rights standards, ensuring surveillance is legal, necessary, proportional, and subject to judicial review.

2.Establish independent oversight bodies with authority to audit, investigate, and enforce compliance with human rights in surveillance.

3.Ensure AI and data analytics in surveillance are transparent, explainable, and regularly audited to prevent discrimination.

4.Implement robust data protection frameworks, including consent, strict retention limits, and safeguards against misuse.

5.Promote international cooperation to create binding standards for cross-border surveillance and data sharing in line with human rights.

6.Raise public awareness of privacy, data protection, and surveillance implications to enhance accountability.

7.Integrate “privacy by design” and “ethics by design” into the development of surveillance technologies.

8.Regularly review counterterrorism and surveillance laws to maintain proportionality, transparency, and democratic oversight.

References

Books

1.Ackerman, B. (2014). *We the people: Volume 3: The civil rights revolution*. Belknap Press, Harvard University Press.

2.Bailey, R. (2013). *Surveillance, accountability, and the algorithmic age*. Routledge.

3.Cameron, I. (2021). *National security and the European Convention on Human Rights*. Brill.

4.De Schutter, O. (2014). *International human rights law* (2nd ed.). Cambridge University Press.

5.Doswald-Beck, L. (2011). *Human rights in times of conflict and terrorism*. Oxford University Press.

6.Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

7.Floridi, L. (2013). *The ethics of information*. Oxford University Press.

8.Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.
9.Javvaji, A. (2023). *Artificial intelligence and surveillance: Ethics, policy, and society*. Palgrave Macmillan.
10.Lindau, J.D. (2022). *Surveillance and the Vanishing Individual: Power and Privacy in the Digital Age*. Rowman & Littlefield.
11.Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge, England: Polity Press.
12.Lyon, D., & Zureik, E. (1996). *Computers, surveillance, and privacy*. University of Minnesota Press.
13.Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press.
14.Malanczuk, P. (2011). Information and communication, freedom of. In *Max Planck Encyclopedia of Public International Law*. Oxford University Press.
15.Solove, D. J. (2010). *Understanding privacy.* Harvard University Press.
16.Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Chapters in Books

1.Matzner, T. (2018). Surveillance as a critical paradigm for big data? In A. R. Sætnan, I. Schneider, & N. Green (Eds.), *The politics of big data: Big data, big brother?* . New York, NY: Routledge.
2.Sætnan, A. R. (2018). The haystack fallacy, or why big data provides little security. In A. R. Sætnan, I. Schneider, & N. Green (Eds.), *The politics of big data: Big data, big brother?* (pp. 21–39). Routledge.

Journal Articles

1.Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy, 3*(5), 1–23.
2.Bonnefont, A. (2024). Human rights implications of the use of new and emerging technologies in the national security space. *Global Centre for Cybersecurity and Emerging Technologies*.
3.Bernot A (2022) Transnational state-corporate symbiosis of public security: China's exports of surveillance technologies. International Journal for Crime, Justice and Social Democracy 11(2): 159-173.
4.Balule, B. T., & Otlhogile, B. (2015). Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana. *Statute Law Review, 37*(1), 19–32.
5.Cain, W. (2023). AI emergence in education: Exploring formative tensions across scholarly and popular discourse. *Journal of Interactive Learning Research, 34*(2), 239–273.
6.Chadha, V. (2022). Balancing the privacy v. surveillance argument: A perspective from the United Kingdom. In *Janus.Net, E-Journal of International Relations*, 13(1), 190–203.
7.Cotula, L. (2020). Between hope and critique: Human rights, social justice and re-imagining international law from the bottom up. *Georgia Journal of International & Comparative Law, 48*(2), 473–521.
8.Debbarma, R. (2023). The changing landscape of privacy laws in the age of big data and surveillance. *Rivista Italiana di Filosofia Analitica Junior, 14*(2), 1740–1752.
9.Deeks, A. S. (2018). Predicting enemies. *Virginia Law Review, 104*(8), 1529–1592.

Journal of Babylon Center for Humanities Studies: 2026, Volume: 16, Issue: 1

10.Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review, 14*(3), 441–458.
11.Fletcher, A. (2023). Government surveillance and facial recognition in Australia: A human rights analysis of recent developments. *Griffith Law Review, 32*(1), 30–61.
12.Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology, 30*(1), 9–37.
13.Javvaji, S. (2023). *Surveillance technology: Balancing security and privacy in the digital age. EPRA International Journal of Multidisciplinary Research (IJMR), 9*(7), 178–185.
14.Königs, P. (2022). Government surveillance, privacy, and legitimacy. *Philosophy & Technology, 35*(8), 1–22.
15.Lynch, N. (2024). Facial recognition technology in policing and security—case studies in regulation. *Laws, 13*(3), 35–48.
16.Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19.
17.Mark, S. (2024). Civil rights in the digital age: Privacy, freedom and justice. *Journal of Civil & Legal Sciences, 13*(2), 433–434.
18.Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2023). The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe. *Journal of Human Rights Practice, 16*(1), 397–412.
19.Mavedzenge, A. (2020). The right to privacy v national security in Africa: Towards a legislative framework which guarantees proportionality in communications surveillance. *African Journal of Legal Studies, 12*(3), 360–390.
20.Nandy, D. (2023). Human rights in the era of surveillance: Balancing security and privacy concerns. *Journal of Current Social and Political Issues, 1*(1), 13–17.
21.Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: An in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing, 6*(5), 1–12.
22.Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A, 376*(2133).
23.Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'experimental' proportionality. *Information & Communications Technology Law, 27*(2), 223–250.
24.Partow-Navid, P., & Slusky, L. (2023). The need for international AI activities monitoring. *Journal of International Technology and Information Management, 31*(3), 114–127.
25.Suman, S. (2023). Application of Smart Surveillance System in National Security. *Unity Journal, 4*(01), 317–330.
26.Smith, M., & Mann, M. (2017). *Facial recognition and privacy: Ethical and legal challenges. Computer Law & Security Review, 33*(2), 122–123.
27.Tzanou, M. (2010). The EU as an Emerging 'Surveillance Society': The Function Creep Case Study and Challenges to Privacy and Data Protection. *ICL Journal, 4*(3), 407-427.
28.Veerabhadraiah, C., & Gayathri Bai, S. (2024). Human rights in the digital age: Balancing privacy, freedom, and security. *International Journal of Commerce, Management, Leadership, and Law, 1*(1), 77–89.

29.Wyden, R., Guthrie, C., Dickas, J., & Perkins, A. (2006). Law and policy efforts to balance security, privacy and civil liberties in post-9/11 America. *Stanford Law and Policy Review, 17*, 329–352.
30.Westin, A. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431–453.

United Nations Documents:

1.United Nations. (2022, September 16). *Spyware and surveillance: Threats to privacy and human rights growing, UN report warns*. OHCHR. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report
2.United Nations Human Rights Council. (2017). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (A/HRC/34/60). United Nations. https://undocs.org/A/HRC/34/60.
3.Cannataci, J. A. (2017, February 24). *Report of the Special Rapporteur on the right to privacy* (A/HRC/34/60). United Nations Human Rights Council.
4.Kaye, D. (2015, May 22). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/29/32). United Nations Human Rights Council.
5.United Nations Human Rights Committee. (2014). *Concluding observations on the fourth periodic report of the United States of America (CCPR/C/USA/CO/4).* United Nations.
6.United Nations General Assembly. (2014, January 21). *The right to privacy in the digital age* (A/RES/68/167). United Nations. https://undocs.org/A/RES/68/167.
7.United Nations Human Rights Council. (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights* (A/HRC/27/37, para. 14). United Nations. https://undocs.org/A/HRC/27/37.
8.United Nations General Assembly. (2014). *Promotion and protection of human rights and fundamental freedoms while countering terrorism: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (A/69/397). United Nations. https://undocs.org/A/69/397.
9.Office of the High Commissioner for Human Rights. (2014). *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*. United Nations.
10.Office of the High Commissioner for Human Rights. (2014). *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights.* United Nations.
11.La Rue, F. (2013, April 17). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/23/40). United Nations General Assembly.
12.United Nations Human Rights Committee. (2011, September 12). *General Comment No. 34: Article 19 – Freedoms of opinion and expression* (CCPR/C/GC/34).
13.Human Rights Council. (2011). Report of the Special Rapporteur on the Promotion And Protection of the Right to Freedom of Opinion and Expression. In *Seventeenth Session*, A/HRC/17/27 .United Nations.

14.United Nations. (1990, February 20). *Guidelines concerning computerized personal data files* (Doc. E/CN.4/1990/72). https://www.un.org/documents/ga/res/45/a45r095
15.United Nations Human Rights Committee. (1988). *General comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17).* United Nations.
16.Office of the United Nations High Commissioner for Human Rights. (1988). *CCPR General Comment No. 16: Article 17 (Right to privacy)*. United Nations.
17.United Nations Human Rights Committee. (1983, July 29). *General Comment No. 11: Prohibition of propaganda for war and inciting national, racial or religious hatred (Article 20)*. CCPR General Comment No. 11.
18.Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). (1979). United Nations.
19.International Covenant on Economic, Social and Cultural Rights (ICESCR). (1966). United Nations.
20.United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights (ICCPR). United Nations Treaty Series*, *999*, 171.
21.United Nations General Assembly. (1948). *Universal Declaration of Human Rights (UDHR)* (Resolution 217 A [III]). United Nations.

Cases:

1.*Al-Haramain Islamic Foundation v. U.S. Department of the Treasury*, 660 F.3d 1019 (9th Cir. 2011).
2.*Antonius Cornelis Van Hulst v. Netherlands*, Communication No. 903/1999, U.N. Human Rights Committee, 2000.
3.*Bridges v. South Wales Police* [2020] EWCA Civ 1058 (Court of Appeal).
4.*Gauthier v. Canada*, Communication No. 633/1995, U.N. Doc. CCPR/C/65/D/633/1995 (1999, May 5). United Nations Human Rights Committee.
5.*La Quadrature du Net and Others v. France* (Joined Cases C-511/18, C-512/18, and C-520/18) [2020] ECLI:EU:C:2020:791 (Court of Justice of the European Union).
6.*M.G. v. Germany*, Communications No. 1482/2006, U.N. Human Rights Committee, 2007
7.*Malone v. Metropolitan Police Commissioner* [1979] Ch 344 (Eng.).
8.Peck v. United Kingdom, 36 E.H.R.R. 41 (2003).
9.R v. Causevic [2016] VSC 321
10.*R v. Immigration Officer at Prague Airport and another (Respondents), ex parte European Roma Rights Centre and others (Appellants), UKHL 55* (2004).
11.*R (B. Mohamed) v. Secretary of State for Foreign and Commonwealth Affairs* [2008] EWHC 2048 (Admin) (Eng.).
12.*R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212 (Can.).
13.*Tele2 Sverige AB v. Watson and Others* (Joined Cases C 203/15 and C 698/15) [2016] ECLI:EU:C:2016:970 (Court of Justice of the European Union).
14.*Toonan v. Australia*, Communication No. 488/1992, U.N. Human Rights Committee, 1994.
15.*United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021).
16.*Vissy v. Hungary*, no. 37138/14, § 54, European Court of Human Rights (ECHR), 2016.
17.*Weber and Saravia v. Germany*, no. 54934/00, § 114, European Court of Human Rights (ECHR), 29 June 2006.

Websites

1.African Commission on Human and Peoples' Rights. (2015). *Principles and guidelines on human and peoples' rights while countering terrorism in Africa* (pp. 12–13). African Union. https://www.achpr.org/public/Document/file/English/achpr_principles_guidelines_countering_terrorism_eng.pdf .

2.Brandon.(2023). Free Speech is Under Fire with the Rise in Global Surveillance. Free Speech is Under Fire With the Rise in Global Surveillance | Tuta

3.Human Rights Watch. (2015, August 19). *Egypt: Counterterrorism law erodes basic rights.* Human Rights Watch. https://www.hrw.org/news/2015/08/19/egypt-counterterrorism-law-erodes-basic-rights.

4.Kumar, C. (2023, October 4). *Government Surveillance and the Erosion of the Right to Privacy.* https://www.linkedin.com/pulse/government-surveillance-erosion-right-privacy-chetan-kumar/

5.Makoni, A. (2022, February 16). Facial recognition cameras in New York are reinforcing racist policing, according to new research by Amnesty. POCIT. https://peopleofcolorintech.com/general/facial-recognition-cameras-in-newyork-are-reinforcing-racist-policing-according-to-new-research-by-amnesty/

6.Palmer, D. (2016, June 9). Security versus privacy: There's only going to be one winner. *ZDNet*. https://www.zdnet.com/article/security-versus-privacy-theres-only-going-to-be-one-winner/.

7.Ryan-Mosley, T. (2022, February 14). A new map of NYC's cameras shows more surveillance in Black and Brown neighborhoods. *MIT Technology Review*. https://www.technologyreview.com/2022/02/14/1045333/map-nyc-cameras-surveillance-bias-facial-recognition/

8.Savov, I. (2016). The Collision of National Security and Privacy in the Age of Information Technologies .European Police Science and Research Bulletin · Issue 15. Bibliotecas: Centro de Análisis y Prospectiva y Academia de Oficiales de la Guardia Civil catalog › Details for: European Police Science and Research Bulletin.

9.Wheatley, M. C. (2024). Ethics of surveillance technologies: Balancing privacy and security in a digital age. *Premier Journal of Data Science*. https://premierscience.com/pjds-24-359/

Reports:

1.Bonnefont, A. (2024). *Human Rights Implications of the Use of New and Emerging Technologies in the National Security Space*. Global Centre for Cybersecurity and Emerging Technologies.

2.Human Rights Watch. (2019). *China's algorithms of repression.* Human Rights Watch.

3.McGregor, L., Fussey, P., Murray, D., & Ng, V. (2018). Submission to OHCHR: The right to privacy in the digital age. Essex University Human Rights Centre.

4.Toulson, R. (2007, February 9). *Freedom of expression and privacy*. (Paper presented at Association of Law Teachers Lord Upjohn Lecture. London).

5.Vice-President Ammoun. (1971). Separate opinion. In *Legal consequences for states of the continued presence of South Africa in Namibia (South West Africa), Advisory Opinion* (ICJ Rep. 1971.

6.Wamala, F. (2011, September). *ITU national cybersecurity strategy guide*. International Telecommunication Union

7.Ziolkowski, K. (Ed.). (2013). *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy*. NATO Cooperative Cyber Defence Centre of Excellence.

Journal of Babylon Center for Humanities Studies: 2026, Volume: 16, Issue: 1