EVALUATING THE EFFECTIVENESS OF DATA PRIVACY LAWS IN INDIA IN MITIGATING CYBERCRIME AND PROTECTING CITIZENS

Dr. Abhishek Kumar Tiwari, Prof., Faculty of Law, University of Lucknow

Amit Kumar Mishra, Research Scholar, Faculty of Law, University of Lucknow

ABSTRACT

In a time marked by global digital interconnectivity, the rapid escalation of cybercrime has compelled governments across the world to establish extensive surveillance frameworks and enact stringent cybersecurity policies. Although such measures aim to safeguard national interests and preserve public order, they give rise to a profound constitutional and ethical dilemma: how can democratic states uphold robust cybersecurity without infringing upon fundamental rights such as personal autonomy and freedom of speech, and due process? This study opens with an analysis of contemporary surveillance technologies—enabled by artificial intelligence, biometric identification, and large-scale data collection—as instruments of both governmental oversight and commercial exploitation. Though frequently framed as measures of protection, these digital systems increasingly obscure the boundary between legitimate security governance and encroachment upon civil liberties. The second section explores how, in the absence of transparency and oversight, surveillance tools are often weaponised against dissenters, journalists, minorities, and civil society—undermining democratic values and eroding public trust under the pretext of national security. The third section interrogates the prevailing global governance gap. Although frameworks like the International Covenant on Civil and Political Rights (ICCPR) and the EU's General Data Protection Regulation (GDPR) seek to articulate digital rights norms, enforcement remains uneven and jurisdictionally fragmented. Such inconsistency fosters conditions in which digital authoritarianism can thrive, often legitimised through the rhetoric of national security imperatives. To conclude, the paper supports a cybersecurity model grounded in human rights, legal safeguards, and democratic checks, ensuring that national security efforts do not come at the expense of individual freedoms in a surveillance-driven era.

Keywords: Cybersecurity, Surveillance Technologies, Civil Liberties, Digital Authoritarianism, Human Rights, National Security.

INTRODUCTION

In today's digital era, the protection of individual freedoms demands that both state authorities and private entities operate under conditions of transparency, accountability, and measured regulation. Frank La Rue, former UN Special Rapporteur on Freedom of Expression.[1]

The 21st-century digital revolution has profoundly transformed the landscape of communication, governance, economic exchange, and public engagement. As societies grow increasingly dependent on digital ecosystems and data-centric technologies, cyberspace has evolved into a domain marked by both immense potential and significant vulnerabilities. The dramatic escalation of cybercrime—including identity theft, ransomware attacks, financial scams, cyberterrorism, disinformation operations, and digital espionage—has driven governments to develop expansive surveillance frameworks and implement comprehensive cybersecurity legislation. And all these are meant to safeguard national security and maintain public order, they also raise significant constitutional and ethical concerns: how can democracies uphold robust cybersecurity without compromising core civil liberties like the right to privacy, free expression, and due process? The present war between national security and individual liberty forms the core of contemporary digital governance debates. The proliferation of surveillance technologies—spanning biometric verification, facial recognition, predictive algorithms, and large-scale data collection—has increasingly obscured the boundary between lawful state authority and unwarranted intrusion. This paper investigates the development and utilization of contemporary surveillance technologies—ranging from artificial intelligence (AI) and biometric identification systems to predictive analytics and mass data storage frameworks—as dual instruments of state authority and corporate commodification. Yet, they all are framed as tools for safeguarding public authority and ensuring national security, they increasingly raise concerns over the encroachment of state power into citizens' private lives. In India, initiatives such as the Central Monitoring System (CMS), NATGRID, and the Aadhaar framework grant authorities unfettered access to personal communication and biometric data, operating within a legal environment often condemned for its lack of transparency, inadequate judicial oversight, and absence of meaningful approval. The Supreme Court's ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India* [2] formally

[1] Frank La Rue, *Special Rapporteur on Freedom of Expression*, United Nations Human Rights Council.
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

recognized a right to privacy as a facet of Article 21 of the Indian Constitution, stipulating that any encroachment on this right must meet the stringent tests of legality, necessity, and proportionality. Nevertheless, subsequent revelations—particularly those surrounding the Pegasus spyware—have laid bare the disconnect between judicial principles and executive actions.[3]However, subsequent developments—particularly the exposure of the Pegasus spyware surveillance program—have highlighted a significant way between the legal framework established by the Court and the actions of the executive. The absence of an exhaustive data protection regime, despite the enactment of the Digital Personal Data Protection Act, 2023[4], continues to vest the state with disproportionate discretion, thereby eroding the very safeguards that the Puttaswamy ruling sought to ensure. Across the globe, similar concerns regarding privacy and surveillance have emerged. In *Carpenter v. United States*,[5] the U.S. Supreme Court ruled that the warrantless acquisition of law enforcement data infringes upon the Fourth Amendment's protection against unreasonable searches. In a comparable vein, the European Court of Human Rights, in *Big Brother Watch v. United Kingdom*[6] , determined that mass surveillance practices conducted without adequate oversight violate the right to privacy under Article 8 of the European Convention on Human Rights. These rulings collectively highlight the necessity for surveillance systems that operate with clarity, transparency, and respect for individual rights. In India, surveillance practices and internet shutdowns disproportionately monitor, intimidate, and suppress the voices of journalists, human rights advocates, political opposers, and vulnerable group.The Supreme Court's ruling in *Anuradha Bhasin v. Union of India* [7] affirmed that both freedom of speech and attainment to access the internet are protected under Article 19(1)(a) of the Constitution. Nevertheless, internet disruptions and content takedowns continue to occur with minimal judicial oversight, bringing attention to the adequacy of enforcement mechanisms. Shoshana Zuboff's[8] concept of "surveillance capitalism" captures the growing fusion between state power and private tech corporations. Within this system, personal information is transformed into a lucrative asset, frequently extracted and profited from without the explicit approval of the individuals involved. Technology Behemoths like Facebook, Google, and Amazon are key players in the large-scale gathering, processing, and privatisation of personal information,

[3] Pegasus, *A Spyware Case Review*, *The Indian Express* (May 2021).
[4] Digital Personal Data Protection Act, 2023, (India).
[5] Carpenter v. United States, 585 U.S. ___ (2018).
[6] Big Brother Watch v. United Kingdom, European Court of Human Rights (2021).
[7] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[8] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

driving both governmental surveillance efforts and corporate data profiling activities. This convergence of public and private surveillance systems not only compromises individual privacy but also endangers the integrity of democratic processes, ultimately eroding the foundation of individual autonomy.

In authoritarian or semi-democratic regimes, the lack of strong legal protections amplifies the risks posed by surveillance often leading to its misuse for political control. The implementation of China's Social Credit System, Russia's Sovereign Internet Legal rules, and the large-scale deployment of facial recognition technologies in global countries such as Turkey and Egypt stand as key areas of the international spread of digital authoritarian practices.[9] In these regimes, surveillance goes beyond national security concerns, functioning as a tool for political repression and societal control. These tactics frequently sidestep constitutional safeguards, stifling free expression and undermining democratic accountability.

Although various international frameworks aim to protect digital rights, their enforcement remains uneven and often swayed by political considerations. Under the ICCPR,[10] especially Articles 17 and 19, individuals are afforded protection against arbitrary privacy infringements and are entitled to the right to free expression. Furthermore, UN General Comment No. 16 regarding Article 17 underscores that any surveillance activities should be carried out with the foundational principles of legality, necessity, and proportionality.

However, many countries adopt limited interpretations of these principles, undermining their global relevance. The GDPR in the European Union, often make with its comprehensive, rights-based framework, featuring key provisions like right to be forgotten (Article 17),[11] data minimization, and purpose limitation. Although the GDPR provides a robust framework, its international carried out has been sluggish, with many countries, including India, still in the process of developing comparable regulatory systems.

Moreover, the extraterritorial reach of digital surveillance introduces additional challenges in terms of accountability. The Snowden revelations[12] exposed how the U.S. NSA, through programs like PRISM and XKeyscore, conducted far-reaching surveillance on foreign citizens

[9] China's Social Credit System, Chinese State Media (2021).
[10] International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 (1966).
[11] UN General Comment No. 16, Article 17, ICCPR, (1988).
[12] *The Guardian*, "Snowden Leaks," (June 2013) https://www.theguardian.com/world/the-nsa-files [Last visited on: July 31, 2025].

without adhering to due process.[13] Though often justified as essential for national security, these actions conflict with international human rights principles and erode global confidence in cross-border data exchanges.

In Schrems II (CJEU, 2020)[14], the EU-U.S. Privacy Shield Framework was struck down, highlighting the insufficient protections against surveillance by the U.S. government.This ruling signals a shift toward increased judicial recognition that the regulation of international digital platforms must be based on multilateral legal standards that uphold individual rights worldwide, rather than following the interests of single national policies. In light of the points discussed, this paper suggests a cybersecurity framework grounded in human rights. Such a rights-centered model demands that surveillance and data management policies meet the fundamental criteria of legality, necessity, and proportionality, as affirmed by the Puttaswamy ruling and reinforced by global legal norms. Additionally, this framework must implement solid institutional safeguards, including autonomous data protection authorities, well-defined judicial oversight processes, and mechanisms that ensure accountability to the publicThe Indian context offers both challenges and opportunities in the area of digital rights and surveillance. While laws like the Digital Personal Data Protection Act, 2023, represent progress, notable gaps remain, especially regarding enforcement autonomy, user rights protection, and the establishement of effective remedies. The lack of parliamentary oversight over intelligence agencies are some urgent institutional reform to safeguard against the misuse of surveillance power.Moreover, legislative frameworks such as the Information Technology Act, 2000[15], and the Indian Telegraph Act, 1885[16], require substantial reform to ensure with constitutional rights and global human rights norms.A unified global framework—perhaps through a binding United Nations convention on digital rights—could help standardize surveillance practices and data protection norms , all while respecting national sovereignty. While bodies like the OECD, G20, and UNHRC have initiated conversations on this front, the absence of binding legal instruments has hindered meaningful advancements.[17]

Ultimately, fostering digital literacy, supporting civil society advocacy, and encouraging

[13] *The Guardian*, "PRISM and XKeyscore Programs," (June 2013) https://www.theguardian.com/world/2013/jun/07/nsa-prism-surveillance-program [Last visited on: July 31, 2025]
[14] *Schrems II*, CJEU Case C-311/18 (2020).
[15] Information Technology Act, 2000, No. 21 of 2000, § 2 (India).
[16] Indian Telegraph Act, 1885, No. 13 of 1885, § 4 (India).
[17] *OECD*, *Guidelines on the Protection of Privacy*, OECD (2013).

judicial activism are key to ensuring accountability. A knowledgeable public, conscious of their digital rights, combined with a judiciary that diligently defends those rights, is essential for maintaining the democratic principles of the digital sovergnity.

A contemporary challenge extends far beyond the fight against cybercrime or safeguard of national cybersecurity. It entails achieving these goals while safeguarding democratic values like liberty, dignity, and accountability. While surveillance technologies play a vital role in effective governance, their use must be confined to a constitutional outline that places human rights above the convenience of executive power.As this paper argues, a rights-based framework built on the principles of legality, necessity, proportionality, and transparency is essential for long-term progress. Without embedding human rights into digital governance, societies may trade their freedoms for an illusory sense of safety, thus undermining the very principles they seek to uphold.

Surveillance Without Oversight — Threat to Democracy and Civil Liberties

The rapid expansion of surveillance technologies in the present area of digital world has changed the dynamic between the state and its citizens. Initially used for enforcing law and order, these digital space become integral to the structure of modern governance. Across various jurisdictions, governments justify the use of these tools by citing concerns over terrorism, cybersecurity, and civil unrest[18]. However, this transformation warrants a critical review of the legal, ethical, and democratic implications of these practices, particularly within constitutional democracies.[19] However, the unchecked and opaque use of surveillance technologies, without proper legal and institutional safeguards, represents a serious threat to civil liberties and democratic governance.[20] Despite being a democracy, the Indian state has adopted expansive surveillance methods, which remain largely unregulated by a comprehensive legal framework.[21] Consequently, fundamental constitutional rights, including the right to privacy, freedom of expression, and due process, are at risk of erosion and misuse[22]. The digital transformation of surveillance has redefined the scale and scope of state monitoring

[18] The Guardian, "Snowden Leaks," (June 2013) https://www.theguardian.com/world/2013/jun/06/nsa-top-secret-programs.
[19] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001).
[20] James Q. Whitman, *Harsh Justice: Criminal Punishment and the Widening Divide Between America and Europe* (Oxford University Press, 2003).
[21] Sidharth Yadav, "Surveillance in India: Legal and Ethical Implications" *Journal of Indian Law and Society* (2021) 12 JILS 45.
[22] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

practices. Modern surveillance now comprises extensive data mining operations that include the interception of emails and mobile communications, real-time tracking of physical movement, analysis of biometric records, and surveillance of online presence. This transformation is driven by the convergence of advanced technologies—artificial intelligence, big data analytics, and cloud computing—that collectively empower governments to conduct granular, continuous, and often automated surveillance of individual behaviour on an unprecedented scale. If we talk about Indian context, this technological shift is exemplified by the establishment of systems such as the Central Monitoring System (CMS), the Network Traffic Analysis System (NETRA), and National Intelligence Grid (NATGRID). [23]While officially framed as instruments for combating terrorism and maintaining internal security, these systems operate within an opaque legal framework and without independent oversight. This institutional vacuum enables unchecked executive power, thereby rendering the surveillance apparatus vulnerable to abuse and the suppression of political dissent. The legal architecture underpinning surveillance in India is both antiquated and insufficient, failing to reflect the constitutional and technological developments of the contemporary era. The Indian Telegraph Act of 1885, along with the Information Technology Act of 2000, continues to form the statutory basis for interception and monitoring. [24]Notably, Section 5(2) of the Telegraph Act [25]permits interception of communications on grounds of "public emergency" or "public safety," terms that remain undefined and ambiguous. Critically, the provision does not mandate prior judicial authorisation, leaving significant room for executive overreach. Similarly, Section 69 of the Information Technology Act, 2000[26], empowers the government to capture, observe, or decode digital data.However, the implementing rules—particularly the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009—lack provisions for independent or judicial oversight, thereby centralising power within the executive.

Although the Supreme Court in *K.S. Puttaswamy v. Union of India* (2018)[27] introduced

[23] Ministry of Home Affairs, *"Central Monitoring System (CMS), National Intelligence Grid (NATGRID), and Network Traffic Analysis System (NETRA)"*, Government of India, accessed 31 July 2023, https://www.mha.gov.in/sites/default/files/InformationOnCmsNatgridNetra_0.pdf.
[24] Indian Telegraph Act, 1885; Information Technology Act, 2000, Ministry of Electronics and Information Technology, Government of India, accessed 31 July 2023, https://www.meity.gov.in/content/information-technology-act.
[25] Indian Telegraph Act, 1885, Section 5(2), accessed 31 July 2023, https://indiankanoon.org/doc/1171854/.
[26] Information Technology Act, 2000, Section 69, accessed 31 July 2023, https://www.legalserviceindia.com/legal/article-2923-information-technology-act-2000.html.
[27] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

restrictions on Aadhaar's mandatory use, it failed to fully grapple with the broader implications of biometric surveillance and state overreach. India's surveillance framework is significantly compromised by the lack of independent oversight mechanisms. In contrast to jurisdictions such as the United States, which employs the Foreign Intelligence Surveillance Court (FISC), and the United Kingdom, which has instituted the Investigatory Powers Tribunal to review state surveillance activities, India relies primarily on executive-led Review Committees. Instead, surveillance authorisations are evaluated by Review Committees comprised solely of executive functionaries, bringing serious attention, lack of transparency, and the erosion of checks and balances essential to democratic governance.

The absence of effective checks and balances has facilitated executive overreach, leading to the gradual erosion of constitutionally protected rights. This has been exacerbated by the growing deployment of real-time surveillance technologies, including Facial Recognition Technology (FRT), social media intelligence tools, and AI-based predictive policing systems. The absence of public consultation, legislative debate, or independent audit mechanisms in the deployment of such tools reflects a deeper crisis of democratic accountability in the digital governance landscape. India's judiciary has played an essential, albeit limited, role in defining the constitutional contours of surveillance. In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court laid down a doctrinal framework requiring any infringement on privacy to match the tests of legality, necessity, and proportionality. Similarly, in *PUCL v. Union of India* (1997), [28]the Court attempted to humanise surveillance law by introducing procedural constraints on telephone tapping, such as mandatory record-keeping and authorisation by senior officials. However, in the absence of institutional enforcement mechanisms, these safeguards have often remained normative rather than operational. Nevertheless, in the absence of institutional enforcement and independent review bodies, the procedural safeguards articulated by the judiciary often remain aspirational rather than operational. The 2021 *Pegasus* revelations highlighted the potential for state surveillance to operate beyond the bounds of constitutional accountability. Allegations that sophisticated spyware was deployed against civil society actors prompted the Supreme Court to initiate an independent inquiry, during which it reaffirmed that national security considerations cannot be used to bypass judicial scrutiny. [29]Similarly, in *Anuradha Bhasin v. Union of India* (2020)[30], as the supreme court advanced the

[28] PUCL v. Union of India, (1997) 1 SCC 301
[29] Pegasus Spyware Scandal, *The Wire*, 2021, accessed 31 July 2023, https://thewire.in/technology/pegasus-project-global-surveillance.
[30] Ibid.

doctrine of proportionality by holding that internet access is foundational to the exercise of Article 19 freedoms, thus reinforcing the imperative of rights-based constraints on digital governance. India's surveillance infrastructure continues to evolve through the rapid expansion of state-controlled technological systems. The Central Monitoring System (CMS) [31]permits direct interception of communications by law enforcement agencies, effectively circumventing telecom service providers and eliminating intermediary safeguards. Although proposals such as the Social Media Communication Hub were ultimately withdrawn due to public outcry, they signal a growing state inclination toward pervasive digital monitoring. Furthermore, Facial Recognition Technology (FRT)[32] has already been deployed in multiple urban areas, despite mounting empirical evidence of algorithmic bias and its disproportionate impact on vulnerable and marginalised populations.

The impact of India's expanding surveillance ecosystem is deeply uneven, disproportionately affecting marginalised communities, political dissenters, journalists, and human rights defenders. Notably, during the anti-CAA-NRC protests, surveillance technologies were reportedly employed to monitor and criminalise Muslim youth and protest organisers. [33]During the anti-CAA-NRC demonstrations, digital surveillance mechanisms were reportedly used to identify and prosecute Muslim protesters, raising questions of selective targeting and communal profiling. In the *Bhima Koregaon* case,[34] revelations that malware may have been used to implant false evidence on the devices of arrested activists challenge the very foundation fundamentals of legal order and the entitlement to an impartial trial. Beyond individual cases, this pervasive surveillance apparatus instils widespread fear, prompting self-censorship and curbing civic mobilisation—ultimately undermining the democratic values safeguarded under Articles 14, 19, and 21 of the Indian Constitution.[35]

A comparative analysis of global surveillance and data privacy frameworks underscores the considerable deficiencies within India's current legal structure regarding data governance. The European Union's General Data Protection Regulation (GDPR), emphasizing the right to

[31] Central Monitoring System, *The Hindu*, 8 July 2013, https://www.thehindu.com/news/national/central-monitoring-system-for-intercepting-communication/article4863621.ece (accessed 31 July 2023).
[32] Facial Recognition Technology and its Impact, *The Wire*, 16 February 2020, https://thewire.in/technology/facial-recognition-surveillance-india (accessed 31 July 2023).
[33] Surveillance and Marginalized Communities, *The Wire*, 18 December 2019, https://thewire.in/rights/surveillance-ca-anrc-muslim-protesters (accessed 31 July 2023).
[34] Bhima Koregaon and the Use of Malware, *Frontline*, 5 October 2020, https://frontline.thehindu.com/india/article32089303.ece (accessed 31 July 2023).
[35] Constitution of India, Article 14, 19, and 21, https://indiankanoon.org/doc/1185865/ (accessed 31 July 2023).

control one's personal data and privacy. The GDPR enforces rigorous standards, including the necessity for transparent data usage purposes, explicit consent from individuals, and oversight by independent regulatory authorities. While India has made strides in developing data protection laws, its current framework lacks the robust mechanisms present in the GDPR, leading to concerns over insufficient protections against privacy violations and a lack of independent oversight in the data governance process.Likewise, The United States uses privacy safeguards like the Privacy Act of 1974[36] and the FISA regime, which subject surveillance activities to judicial review. India's status as a party to the International Covenant on Civil and Political Rights (ICCPR) imposes clear obligations, particularly for prevention of arbitrary surveillance and safeguarding the right to free expression, as enshrined in Articles 17 and 19, respectively. An independent oversight body, comprising members of the judiciary and subject-matter experts, should be constituted to scrutinise both ex ante and ex post surveillance measures.

Global Normative Gaps and the Rise of Digital Authoritarianism

The advent of the digital era has fundamentally reshaped the architecture of governance, embedding surveillance as a core instrument of statecraft. While emerging technologies have augmented the state's ability to address cybercrime, streamline governance, and respond to crises, they have simultaneously conferred expansive capabilities to monitor, profile, and exercise control over populations. This duality presents a critical dilemma—how to harness the utility of digital tools without subverting democratic principles and civil liberties. What renders this trajectory particularly perilous is the conspicuous absence of binding and harmonised global norms capable of regulating state surveillance and safeguarding digital rights. Without strong international legal oversight, digital authoritarianism has flourished, taking shape as the calculated exploitation of digital infrastructure to cement authoritarian control, usually justified disguised under the guise of national security and public welfare.

Through key instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the European Union's General Data Protection Regulation (GDPR), international human rights law means to provide a normative structure for defending digital rights.Article 17 of the ICCPR protects against infridgement with privacy, while Article 19 guarantees the right to freedom of expression. These principles are reinforced by the UN Human Rights

[36] Privacy Act of 1974, 5 U.S.C. § 552a, https://www.justice.gov/opcl/privacy-act-1974 (accessed 31 July 2023).

Council in Resolutions 68/167 and 69/166, which affirm that digital rights are to be treated on par with offline rights.Though these instruments hold normative value, their enforceability is limited, and their impact is often diminished by state-driven interpretations of sovereignty and national security. Despite their normative importance, international frameworks like the ICCPR and GDPR are severely limited in effectiveness due to their non-binding nature. The absence of universal enforcement mechanisms, and jurisdictional limitations. While the GDPR is often hailed as the gold standard in data protection, its scope of application is restricted to the EU and entities that manage the personal data of EU citizens.

There is no global requirement for countries outside the EU to adhere to its principles. Similarly, although the International Covenant on Civil and Political Rights (ICCPR) give important role in human rights law , it is limited by the absence of concrete enforcement mechanisms for its direct application[37].

A growing number of democracies, despite maintaining regular electoral processes, are integrating surveillance techniques that obscure the clear demarcation between lawful state governance and repressive rule.[38] This blurring of lines raises critical questions about the preservation of civil liberties and the role of state power in an increasingly digital age. China's Social Credit System and India's Aadhaar initiative exemplify how state-managed databases can serve as tools for regulating behavior and profiling citizens. In parallel, countries like Russia and the United States are employing advanced technologies such as facial recognition and algorithmic policing, which contribute to a growing surveillance infrastructure. These advancements not only improve state control but also risk reinforcing discriminatory biases and exacerbating social inequalities. Concurrently, nations such as Turkey, Iran, and Egypt utilize digital censorship strategies—ranging from restricting access to online platforms to prosecuting individuals for their online activities—as a means to suppress dissent and restrict public discourse. Such practices not only undermine citizens' access to information but also highlight the growing role of digital technologies in enabling state control over public life and dissenting voices. Governments frequently defend the expansion of digital surveillance under the broad pretext of national security, claiming it is essential for combating terrorism,

[37] United Nations, **International Covenant on Civil and Political Rights (ICCPR)**, 999 U.N.T.S. 171, adopted Dec. 16, 1966, entered into force Mar. 23, 1976, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[38] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (PublicAffairs, 2011); The Guardian, "Digital Authoritarianism: How Surveillance States Are Spreading," available at: https://www.theguardian.com/.

cyberattacks, and organized crime Although these risks are tangible, the use of national security as a blanket justification—lacking precise legal parameters or independent oversight—raises significant ethical and legal concerns, particularly regarding the potential for overreach and the infringement on individual freedoms.[39] The unchecked proliferation of surveillance technologies fosters an environment in which democratic safeguards are progressively eroded. While such measures may begin with legitimate concerns for national security, they increasingly become instruments of political control, curbing dissent and limiting fundamental freedoms. This shift not only endangers individual rights but also undermines the very principles that sustain democratic societies. Digital authoritarianism flourishes in regions where global protections for human rights are insufficiently robust. In response, the international community must move beyond aspirational guidelines and adopt legally binding frameworks that safeguard digital rights, mandate independent oversight, and hold violators accountable. This shift is crucial for upholding fundamental freedoms in the digital era. Critical steps include enforcing the principles of legality and proportionality, regulating the international trade of surveillance technologies, and ensuring cross-border accountability for violations.[40]

The unchecked expansion of surveillance technologies, coupled with the absence of strong global standards, has driven the rise of digital authoritarianism. Although legal frameworks such as the ICCPR and GDPR are in place, their enforcement is weak, and jurisdictional gaps provide states with opportunities to bypass their human rights commitments, often in the name of national security.[41]

The rapid advancement of surveillance technologies in today's digital landscape calls for a critical reassessment of global cybersecurity frameworks. While the intention to counter cybercrime, espionage, and terrorism is legitimate, there is an alarming trend where such innovation leveraged for authoritarian purposes.

This shift highlights pressing challenges related to democratic oversight, the integrity of the rule of law, and the gradual erosion of civil liberties. In many democracies, the frameworks

[39] "Security vs. Privacy: The Surveillance Dilemma," *Amnesty International*, accessed July 31, 2025, https://www.amnesty.org/en/latest/research/2020/03/security-vs-privacy-surveillance/.
[40] Regulating Surveillance Technologies: A Path to Global Accountability," *Amnesty International*, accessed July 31, 2025, https://www.amnesty.org/en/latest/research/2023/05/toward-global-oversight-surveillance-technology/.
[41] General Data Protection Regulation (GDPR), European Union, 2016, accessed July 31, 2025, https://gdpr.eu/.

designed to govern surveillance have failed to evolve alongside technology, which has, in turn, allowed executive power to expand unchecked. This section contends that the development of a cybersecurity framework centered around human rights is critical for aligning national security objectives with constitutional guarantees and global legal norms. This transformation must be grounded in a legally binding international digital rights treaty, reinforced through multilateral frameworks, and guided by the "Necessary and Proportionate" principles.[42]

The governance of digital rights remains fragmented across several international treaties, regional agreements, and national laws, leading to a lack of consistency and enforcement. Such a framework would establish clear, universally applicable standards for privacy, data protection, and surveillance practices, ensuring that individuals' rights are preserved as digital technologies continue to evolve. In doing so, it would provide a structured approach to balancing security concerns with the protection of fundamental freedoms in the digital landscape. While the ICCPR enshrines crucial protections for privacy (Article 17) and freedom of expression (Article 19), these provisions were conceived long before the advent of widespread digital surveillance and profiling technologies.[43]

This limitation underscores the fragmented and often inconsistent approach to global digital rights protection, revealing the challenges inherent in establishing a coherent and universally applicable framework for privacy and data security.However, the enforceability of the GDPR is restricted to EU member states and entities processing the data of EU citizens, thus highlighting the fragmented and inconsistent landscape of global digital rights protection. This regulatory gap underscores the pressing need for an internationally binding treaty that establishes clear and consistent digital rights standards . Such an instrument would promote consistency in the safeguard of digital rights, bridging legal divides and ensuring comprehensive safeguards across jurisdictions.

Such a treaty must comprehensively codify rights related to data privacy, algorithmic transparency, access to encryption, and protections against indiscriminate mass surveillance. It must also establish clear parameters for permissible restrictions on these rights, grounded in the foundational principles of global human rights law, including legality, necessity, and

[42] *Global Principles on National Security and the Right to Privacy*, available at: https://necessaryandproportionate.org.,last accessed on 31 st July 2025.
[43] Digital Surveillance and Human Rights: The Need for International Standards," United Nations Human Rights Office (2021), available at: https://www.ohchr.org.

proportionality, to prevent overreach and safeguard individual freedoms. To ensure meaningful implementation, the treaty must include robust enforcement mechanisms, such as independent oversight bodies and accessible channels for judicial redress. Such measures are essential to convert the treaty's aspirational principles into binding obligations, ensuring both compliance and the protection of individual rights on a global scale.

A core component of a human rights-based cybersecurity framework is the adoption of the "Necessary and Proportionate" principles, which provide a thorough legal structure for evaluating the legality of surveillance activities.[44]These principles, arising from international civil society coalitions and endorsed by United Nations bodies, require that surveillance be grounded in law, necessary within a democratic framework, proportionate to its intended objectives, and subject to prior independent approval and meaningful oversight.

CONCLUSION

As we conclude this exploration into the complex intersections of digital security, state surveillance, and fundamental freedoms, a vital issue resurfaces the digital revolution has redefined both the scope of modern security threats and the ways in which authority operates and individual rights are challenged. With cyber dangers—such as hacking, digital espionage, misinformation, and attacks on critical systems—becoming increasingly pervasive, governments are justified in deploying defensive mechanisms. They must instead be harmonised with democratic principles, the supremacy of law, and dignity for human rights.

This inquiry addresses the aforementioned dilemma by first analysing the architecture of modern surveillance technologies, such as artificial intelligence (AI)-driven systems, biometric recognition tools, and expansive data mining operations. Justified primarily for enhancing national security and operational efficiency, these frameworks operate in two capacities—empowering government authorities but also avenues through which private companies profit from data commodification. While framed as precautionary measures for protection, these digital infrastructures progressively erase the divide between lawful regulation and unwarranted interference, making it harder to differentiate between safeguarding security and infringing on civil rights.

[44] International Principles on the Application of Human Rights to Communications Surveillance, *Necessary and Proportionate Principles*, available at: www.necessaryandproportionate.org (accessed July 31, 2025).

Additionally, the powerful influence of multinational tech corporations, along with the absence of binding international laws on cross-border data management, exacerbates the issue significantly. The commodification of personal data, algorithmic profiling, and predictive law enforcement actions are frequently conducted in the absence of clear legal boundaries, thereby making it difficult to enforce meaningful democratic oversight and accountability.