

Beyond Encryption: Quantum-Ready Surveillance and the Constitutional Limits of the Digital State

Dr. Vijaykumar Shrikrushna Chowbe¹, Miss Smita Chandrabhan Thool²

“Privacy is the ultimate expression of the sanctity of the individual.”

DOI: <https://doi.org/10.51583/IJLTEMAS.2026.150900037>

Received: 16 September 2026; Accepted: 21 September 2026; Published: 03 October 2026

ABSTRACT

The architecture of surveillance is approaching a profound technological and normative transition. Artificial intelligence can already infer, classify and monitor human behaviour at unprecedented scale; biometric identification, large-scale data integration and algorithmic inference can expand the State's capacity to identify, correlate and profile individuals. Quantum computing introduces a different but related challenge by threatening the cryptographic assumptions upon which the confidentiality and authenticity of digital life have long depended. Post-quantum cryptography (PQC) responds principally to that cybersecurity problem: it protects confidentiality, authentication and integrity against quantum-capable adversaries, but does not itself enlarge the State's capacity to collect or infer information. This article therefore uses “quantum-ready surveillance” to describe surveillance infrastructures in which capability-expanding technologies operate within quantum-resilient security architectures, while keeping those functions analytically distinct.

The study argues that quantum readiness presents a governance paradox, not because PQC itself creates new surveillance powers, but because more durable and quantum-resilient infrastructures may secure and preserve surveillance data generated through AI, biometrics, interoperable databases and large-scale collection. In an environment of “harvest now, decrypt later,” algorithmic decision-making and increasingly integrated governmental information systems, the constitutional problem concerns both the expansion of surveillance capability and the security architecture within which collected information is transmitted, authenticated and retained. Drawing upon India as the principal case study, with the United States and European Union as structured comparators, the article evaluates these developments against legality, necessity, proportionality, transparency, explainability and independent oversight.

The article finds that the principal deficit is not merely technological preparedness but governance preparedness. Existing legal regimes remain fragmented, territorially bounded and institutionally uneven, while quantum-resilient digital infrastructures and AI-enabled surveillance operate across borders and institutional boundaries. It therefore advances an eight-component rights-centred model: technological resilience and crypto-agility; constitutional legality; privacy and rights by design; accountable AI; institutional accountability; risk-tiered governance; international interoperability; and technological equity. These components are operationalised through an integrated governance cycle—Resilience → Legality → Necessity → Privacy by Design → Risk Classification → Authorization → Auditability → Independent Oversight → Redress → Periodic Review → International Interoperability. Quantum security and human freedom need not be competing objectives; legitimacy depends upon ensuring that a quantum-secure State remains constitutionally restrained and democratically accountable.

Keywords: Quantum-Ready Surveillance; Post-Quantum Cryptography (PQC); Artificial Intelligence and Surveillance; Privacy and Human Dignity; Constitutional Proportionality; Ethical Governance;]

INTRODUCTION

The twenty-first century has transformed the relationship between national security, technological power and individual liberty. Cybersecurity is no longer confined to protecting isolated computer networks from

conventional intrusion; it has evolved into a transnational governance challenge involving critical infrastructure, cloud ecosystems, cross-border data flows, artificial intelligence, state-sponsored cyber operations and increasingly sophisticated forms of digital surveillance. The contemporary threat environment is correspondingly complex. The European Union Agency for Cybersecurity (ENISA), after analysing thousands of publicly reported cybersecurity incidents, identifies ransomware, malware, threats against data, denial-of-service attacks, information manipulation and interference, and supply-chain attacks among the principal contemporary cyber threats, while also observing the continuing influence of geopolitical conflict and state-linked actors upon the cyber threat landscape.³ Such developments have progressively blurred the traditional boundaries between cybersecurity, intelligence gathering and surveillance: the State is increasingly required not merely to respond to completed attacks but to anticipate threats through continuous collection, correlation and algorithmic analysis of digital information.

Against this already contested background, quantum computing introduces a qualitatively different dimension to the security–liberty debate. The concern is not simply that quantum computers may increase computational capacity; sufficiently capable quantum systems could undermine widely deployed public-key cryptographic mechanisms upon which the confidentiality and authenticity of contemporary digital communications depend.⁴ NIST therefore warns that information requiring long-term confidentiality is vulnerable even before a cryptographically relevant quantum computer becomes operational, because adversaries may intercept and preserve encrypted information today for future decryption—a strategy commonly described as “harvest now, decrypt later”.⁵ The problem consequently possesses an unusual temporal character: information protected by encryption today may become retrospectively vulnerable tomorrow.

This prospect has accelerated the transition towards post-quantum cryptography (PQC) and quantum-resilient digital infrastructures. Contemporary scholarship accordingly treats the quantum threat as a present cybersecurity problem requiring migration planning before cryptographically relevant quantum computers become available. A critical distinction is necessary at the outset. PQC is a security technology: it protects confidentiality, authentication and integrity against quantum-capable adversaries. It does not, by itself, collect additional information, identify individuals, integrate databases or generate behavioural inferences. Surveillance capability is expanded instead by technologies such as biometric identification, persistent sensing, large-scale data integration and AI-based classification or inference. The constitutional concern arises when those capability-expanding systems are embedded within increasingly durable, interoperable and quantum-resilient infrastructures, because security modernization may preserve and entrench surveillance architectures without supplying the legal safeguards that should govern their use.⁶⁷

States and corporations are therefore preparing quantum-resilient digital systems while simultaneously expanding the use of AI, big-data analytics and biometric technologies. For analytical purposes, this article describes the resulting institutional environment as “quantum-ready surveillance” only where these distinct layers converge: AI, biometrics and data integration determine the capacity to collect, classify or infer information, whereas PQC secures the transmission, authentication and long-term integrity of the infrastructure and data. The term must not be understood to imply that PQC itself expands surveillance reach. The governance paradox is narrower but important: a surveillance system may become more secure and durable against external compromise while remaining excessively intrusive, insufficiently authorised or weakly supervised from a constitutional perspective.⁸⁹¹⁰

This article explores the ethics of quantum-ready surveillance through the lens of international law, constitutional morality, and human rights theory. It asks: How can states reconcile the imperative of securing critical infrastructures with the ethical duty to respect privacy, dignity, and freedom? It further investigates whether PQC and AI-enabled transparency mechanisms—such as explainable AI and blockchain-based logging—can serve not only as technical safeguards but also as tools of ethical legitimacy. By situating technical debates within broader ethical and legal frameworks, this study seeks to contribute to the growing discourse on building secure yet rights-respecting digital futures.

Analytical Methodology and Comparative Design

This article adopts a doctrinal and structured comparative legal methodology. India constitutes the principal case study because the paper's normative recommendations are directed primarily to the constitutional and institutional implications of India's rapid quantum-security transition, including the Digital Personal Data Protection Act, the National Quantum Mission, emerging quantum-safe migration policy and the constitutional proportionality framework developed in Justice K.S. Puttaswamy (Retd.) v. Union of India.¹¹ The United States and the European Union are used as functional comparators rather than as co-equal country studies. They were selected because they represent contrasting regulatory traditions: the United States combines extensive national-security surveillance authority with sectoral privacy controls and institutional oversight, whereas the European Union employs a more rights-centred data-protection and risk-regulation model.

Against this backdrop, governments and corporations are migrating towards quantum-resilient digital infrastructures.¹² These standards are designed to secure key establishment and digital signatures against quantum-capable adversaries. Their relevance to surveillance is infrastructural rather than capability-expanding: PQC can protect stored or transmitted surveillance information and authenticate evidence, but it does not determine whether data should be collected or how individuals should be profiled.

The normative framework is derived from recurring public-law and human-rights principles applicable to technologically mediated surveillance: legality, legitimate purpose, necessity, proportionality, transparency, accountability, independent oversight, effective redress and, where automated systems materially affect individuals, explainability and meaningful human review. The comparison asks how each jurisdiction structures these safeguards around surveillance capability and around the security infrastructure that stores or transmits surveillance information. The methodology deliberately distinguishes descriptive law from critical evaluation and from the authors' normative proposals. Its principal limitation is that quantum-resilient migration and AI regulation are rapidly evolving; the article therefore evaluates the legal and policy position within the stated period and does not claim an exhaustive account of classified surveillance practice or every sector-specific rule.

Parallel to cryptographic migration, AI-driven surveillance has expanded through predictive analytics, biometric identification, anomaly detection and large-scale data correlation. These technologies—not PQC—can increase the reach and inferential power of surveillance. When deployed within PQC-secured infrastructure, the resulting system combines two distinct functions: AI, biometrics and integrated datasets may expand monitoring and inference, while PQC protects communications, stored information and authentication against quantum-capable adversaries. The constitutional risk therefore arises from the surveillance capability of the former and the potential durability and security of the combined architecture, not from any independent surveillance power created by PQC.

The emergence of quantum computing has redefined the stakes of global cybersecurity. Classical cryptographic systems such as RSA, ECC, and Diffie–Hellman have long served as the backbone of digital trust.¹³ Yet, Shor's algorithm demonstrated that once scalable quantum computers arrive, these schemes could be broken in polynomial time, rendering vast troves of encrypted communications vulnerable.¹⁴ This has given rise to a troubling strategy known as “harvest now, decrypt later,” where adversaries intercept and store encrypted data today, anticipating its decryption once quantum capabilities mature.¹⁵ The advent of quantum computing transforms cybersecurity from a problem of protecting present communications into one of long-term informational vulnerability, as data considered securely encrypted today may be harvested, preserved, and retrospectively exposed once quantum capabilities mature.

Against this backdrop, surveillance infrastructures worldwide are evolving into quantum-ready ecosystems. Governments and corporations are investing heavily in post-quantum cryptography (PQC), which offers algorithms like Kyber (for key exchange) and Dilithium (for signatures), standardized by NIST in 2022.¹⁶ These tools promise resilience against both classical and quantum adversaries. However, their integration

into surveillance systems raises a crucial question: can PQC strengthen state security without simultaneously eroding fundamental rights?

The Expansion of AI-Enabled Surveillance

Parallel to cryptographic innovations, AI-driven surveillance has surged. From predictive policing to biometric identification, machine learning models increasingly guide decisions about security and risk.¹⁷ When fused with PQC, AI-enabled surveillance achieves unprecedented reach: it can protect communications against decryption while simultaneously powering expansive monitoring of populations.¹⁸ This dual capacity illustrates the paradox of quantum-ready surveillance: it fortifies state security while amplifying the ethical risks of unchecked observation.

For instance, China's large-scale integration of AI with state surveillance infrastructures demonstrates how technical advances can entrench authoritarian control.¹⁹ In liberal democracies, too, the reliance on AI surveillance has grown—ranging from U.S. counterterrorism monitoring under FISA to EU digital infrastructure monitoring under GDPR-compliant safeguards.²⁰ The question is no longer whether surveillance will expand, but whether it will do so within frameworks that respect privacy and dignity.

Forensic Readiness in Surveillance Systems

In addition to prevention, modern surveillance emphasizes accountability. Forensic readiness—embedding forensic logging and evidence preservation into systems—has become central to ensuring that security actions are both transparent and legally auditable.²¹ Blockchain-based forensic systems allow for tamper-proof evidence chains, while explainable AI (XAI) provides interpretability, enabling courts and regulators to scrutinize algorithmic conclusions.²² When integrated with PQC, these tools ensure that forensic evidence remains resistant to quantum decryption, preserving both technical integrity and legal admissibility.²³ Thus, forensic readiness integrated with PQC and XAI transforms surveillance from a reactive tool into a proactive, trustworthy system that safeguards both security and legal legitimacy.

Global Trends in Quantum-Ready Surveillance

States worldwide are already experimenting with quantum-ready surveillance infrastructures. The EU has launched initiatives under the Quantum Flagship program to explore PQC-enabled secure communications.²⁴ India's Digital Personal Data Protection Act (DPDP, 2023) provides a sovereignty-aware framework, shaping how surveillance and data processing must comply with human rights principles.²⁵ Meanwhile, NATO's Cooperative Cyber Defence Centre of Excellence emphasizes the integration of quantum-resilient tools in its cyber exercises.²⁶ Yet, while these developments enhance security, they also expose a governance vacuum. Without shared ethical frameworks, there is a risk that quantum-ready surveillance will deepen power asymmetries, normalize invasive monitoring, and sideline human rights in the name of security.²⁷ Thus, Quantum-ready surveillance sits at the crossroads of opportunity and risk. On one hand, PQC and AI can safeguard communications and strengthen global defenses; on the other, they can entrench unaccountable surveillance architectures. The challenge is to ensure that resilience against quantum threats evolves hand in hand with respect for fundamental freedoms, creating systems that are both technologically robust and ethically sustainable.

Security Imperatives vs. Human Rights

The promise of quantum-ready surveillance lies in strengthening national security. States argue that advanced monitoring tools are indispensable in protecting critical infrastructures, anticipating cyberattacks, and countering terrorism. The reality of transnational cyber threats—ransomware on hospitals, attacks on power grids, and state-sponsored espionage—makes these claims persuasive.²⁸ Quantum-resilient systems, paired with AI-driven surveillance, allow for faster anomaly detection, predictive threat modeling, and real-time coordination across borders.²⁹ Yet these security imperatives collide directly with human rights frameworks. International law recognizes privacy, dignity, and freedom of expression as foundational.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with privacy, while regional regimes such as the European Convention on Human Rights (ECHR) extend robust protections against disproportionate surveillance.³⁰ The challenge is not whether surveillance is necessary, but whether it is proportionate, accountable, and rights-respecting.

The National Security Argument

Governments frequently invoke national security to justify expanded surveillance. In the U.S., Section 702 of the Foreign Intelligence Surveillance Act (FISA) has enabled the bulk collection of foreign communications, justified as necessary for counterterrorism.³¹ In India, the Aadhaar system and the DPDP Act (2023) grant the state expansive powers to process personal data, framed as essential for governance and digital security.³² Similarly, China's cybersecurity law permits sweeping monitoring of online activity, legitimized as defending sovereignty.³³ Thus, while such frameworks strengthen state capacities, they also illustrate the ethical tension: security becomes an elastic justification, capable of stretching to cover broad and sometimes intrusive forms of surveillance. The ethical question is whether the benefits of quantum-ready security outweigh the risks of normalizing disproportionate state intrusion.

Ultimately, these examples reveal that while national security may justify stronger surveillance powers, in practice it often stretches into a justification for disproportionate intrusion—raising the critical ethical question of how far states can go in the name of quantum-ready security without eroding fundamental rights.”

Human Rights Concerns

Human rights advocates argue that surveillance at quantum scale risks creating “panoptic societies,” where individuals live under constant observation.³⁴ Beyond privacy, such systems can have chilling effects on speech, association, and dissent. For example, predictive policing systems disproportionately target marginalized communities, entrenching systemic bias.³⁵ Similarly, biometric surveillance, if paired with PQC and AI, could lock individuals into permanent systems of identification and control, undermining autonomy.³⁶ International jurisprudence has underscored the importance of proportionality. The European Court of Human Rights, in cases such as *Big Brother Watch v. United Kingdom*,³⁷ ruled that mass surveillance regimes without adequate safeguards violate privacy and freedom of expression.³⁸ These judgments stress that even where surveillance is justified, it must be narrowly tailored, transparent, and subject to oversight.

Reconciling the Divide

Bridging security imperatives with human rights demands governance models that prioritize proportionality and necessity. Legal safeguards must evolve to recognize PQC-signed evidence, AI-driven forensics, and blockchain logging as credible but accountable tools.³⁹ Judicial oversight and independent review boards should function as counterweights to unchecked surveillance power. Equally, public transparency—through audit reports and algorithmic explainability—can mitigate fears of hidden monitoring.

Thus, the tension between state security and human rights is not a binary choice but a matter of balance. Quantum-ready surveillance can strengthen resilience against unprecedented threats, but if left unregulated, it risks undermining the very freedoms it claims to protect. The path forward lies in frameworks that treat security and rights not as opposites, but as co-dependent pillars of ethical governance.

Ethical Frameworks and Case Studies

A rights-based framework emphasizes that privacy, dignity, and autonomy are intrinsic human-rights interests that cannot be reduced to a simple utilitarian calculation. The Universal Declaration of Human

Rights, 1948¹ and Article 17 of the ICCPR protect privacy against arbitrary or unlawful interference. Privacy under Article 17 is not, however, one of the rights expressly listed as non-derogable in Article 4(2) of the ICCPR. The legally relevant point for surveillance analysis is therefore that any interference with privacy must have a lawful basis and must not be arbitrary; necessity, proportionality, safeguards and effective oversight remain central to assessing legitimacy, including during periods of heightened security concern.

Utilitarian Justifications and Their Limits

From a utilitarian perspective, surveillance can be defended as maximizing overall welfare: if monitoring a few individuals prevents large-scale cyberattacks or terrorist incidents, the trade-off appears justified.⁴⁰ For example, predictive policing systems or bulk metadata collection may be seen as proportionate if they avert greater harms. Yet critics note that utilitarian logics often ignore distributive justice. Surveillance regimes tend to disproportionately impact marginalized communities, exposing them to profiling or discriminatory targeting.⁴¹ In quantum-ready systems, where AI and PQC enhance the scope of monitoring, the risk is that efficiency trumps equity, leading to systemic erosion of trust. Utilitarian reasoning, therefore, must be checked by safeguards ensuring fairness and proportionality. Thus, while utilitarian justifications highlight the collective benefits of surveillance, the danger lies in efficiency overwhelming equity—making safeguards of fairness and proportionality indispensable for ethical legitimacy in the quantum era.

Rights-Based Approaches

A rights-based framework emphasizes that privacy, dignity, and autonomy are not contingent goods but intrinsic human rights. The Universal Declaration of Human Rights, 1948⁴² and ICCPR enshrine privacy protections irrespective of utilitarian calculations.⁴³ Under this view, even if surveillance promises greater security, it cannot trample upon non-derogable rights.

European jurisprudence exemplifies this approach. The GDPR, with its strong emphasis on data minimization, consent, and accountability, seeks to embed rights into governance of digital infrastructures.⁴⁴ The European Court of Human Rights in *Big Brother Watch v. UK* (2021)⁴⁵ affirmed that indiscriminate surveillance without safeguards is incompatible with rights to privacy and expression.⁴⁶ Rights-based approaches thus establish ethical boundaries that technology must respect, even under quantum threats.

The comparative component is structured around India as the principal case study and the United States and European Union as functional comparators. The jurisdictions were selected because they illuminate materially different approaches to the relationship between national security, privacy, data governance and technologically assisted surveillance. India provides the article's primary constitutional and policy setting; the United States illustrates a security-oriented surveillance architecture with statutory and institutional oversight mechanisms; and the European Union provides a rights-centred regulatory model combining data protection with risk-based AI regulation. The purpose is therefore not to claim a perfectly symmetrical three-jurisdiction survey, but to use carefully selected comparators to test and refine the governance framework proposed for India and for transnational quantum-resilient systems.

In India, constitutional morality provides a distinct framework. The Supreme Court in *Justice K.S. Puttaswamy v. Union of India*⁴⁷ recognized privacy as a fundamental right, requiring state surveillance to pass the tests of legality, necessity, and proportionality.⁴⁸ Applying these principles to quantum-ready surveillance means the state must justify intrusions with clear legal authority, narrowly tailored measures, and oversight mechanisms.

1 United Nations General Assembly, Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217(III) (10 December 1948), art. 12, available at: Official United Nations – Universal Declaration of Human Rights (last accessed 22 September 2026).

For example, India's DPDP Act, 2023 strengthens state powers in processing personal data, but critics argue that without robust judicial oversight, the balance may tilt towards state control rather than individual liberty.⁴⁹ Constitutional morality thus demands that surveillance, however technologically advanced, be subjected to democratic accountability.

European Union – GDPR and AI Act - The EU provides a contrasting rights-centred model. The GDPR embeds principles of lawfulness, purpose limitation, data minimisation, transparency and accountability. Regulation (EU) 2024/1689 (the Artificial Intelligence Act) entered into force on 1 August 2024 and is being applied through a staged timetable; its risk-based framework is especially relevant to biometric identification and other high-risk or prohibited AI practices. The EU example therefore illustrates how quantum-resilient infrastructure can be governed separately from, but alongside, legal controls directed at AI-enabled surveillance capability.

The governance of emerging surveillance technologies cannot be understood through a single legal model, as states differ considerably in balancing national security, technological efficiency, and individual privacy.⁵⁰ A comparative examination of India, the United States, and the European Union reveals three distinct regulatory approaches—India's evolving data-governance framework, the United States' security-oriented surveillance architecture, and the European Union's rights-centred regulatory model. These jurisdictions therefore provide useful comparative perspectives for assessing how post-quantum cryptography (PQC) may simultaneously strengthen cybersecurity while reshaping the legal and ethical boundaries of state surveillance.

- a) **India – Aadhaar and DPDP 2023** - India's Aadhaar program—world's largest biometric database—has faced scrutiny for potential misuse in surveillance. The DPDP Act, 2023 reinforces state control over data under the banner of security and governance.⁵¹ While PQC may enhance security, critics argue that without stronger checks, such systems risk sliding into centralized surveillance architectures.
- b) **United States – FISA and NSA Surveillance** - The U.S. experience illustrates how national security narratives can expand surveillance. The Snowden revelations exposed bulk collection of metadata under FISA, sparking debates over legality and ethics.⁵² As quantum threats loom, U.S. agencies are moving towards PQC-enabled systems, but concerns persist that enhanced resilience may simply entrench already expansive surveillance powers.
- c) **European Union – GDPR and AI Act** - The EU represents a contrasting model, prioritizing privacy by design. GDPR emphasizes transparency and accountability, while the upcoming AI Act seeks to regulate high-risk AI systems, including biometric surveillance.⁵³ Quantum-ready surveillance in the EU will likely be shaped by these stringent rights-based frameworks, highlighting a different ethical balance.

Global surveillance operates in a fragmented legal landscape. The EU combines the GDPR with the AI Act, which entered into force on 1 August 2024 and is subject to staged application. The United States follows a more sectoral and national-security-oriented model under FISA and related statutes, while India's DPDP Act reflects a sovereignty-conscious data-governance approach whose interaction with surveillance law continues to evolve. The lack of harmonized standards creates regulatory collisions in cross-border data access, evidentiary authentication and accountability. Quantum-resilient cryptography does not itself resolve these legal differences; it makes interoperability, long-term authentication and governance coordination increasingly important.

Governance Gaps and Towards an Ethical Framework

While quantum-ready surveillance promises enhanced security, its deployment exposes deep governance gaps. These gaps are not limited to technology, but extend across law, policy, and ethics—making it urgent to develop a principled framework that balances state security with human rights.

Fragmentation of Legal Standards

Global surveillance operates in a fragmented legal landscape. The EU's GDPR and forthcoming AI Act emphasize privacy and accountability, while the U.S. follows a patchwork model under FISA and sector-specific statutes. India's DPDP Act reflects a sovereignty-conscious approach, but its enforcement capacity remains uncertain.⁵⁴ Meanwhile, China enforces state-centric surveillance under its cybersecurity law. The lack of harmonized standards creates regulatory collisions: evidence admissible in one jurisdiction may be invalid elsewhere, and data transfers remain hostage to localization mandates.⁵⁵ Thus, without international coordination, quantum-ready surveillance risks creating a two-tier system: technologically advanced nations dictating global norms,⁵⁶ while smaller states are left as passive adopters or sites of exploitation.

Accountability Deficits

Even where laws exist, accountability mechanisms are weak. Oversight bodies often lack technical expertise to review AI-driven surveillance or PQC-enabled forensics. Parliamentary committees, data protection authorities, and courts struggle to keep pace with evolving technologies.⁵⁷ Moreover, secrecy justified by national security narrows the scope of public scrutiny.⁵⁸ This opacity undermines trust, especially when surveillance disproportionately targets vulnerable groups.

The Need for Ethical Anchors

Governance must therefore move beyond fragmented compliance to embrace ethical anchors. Principles such as proportionality (intrusions must be necessary and minimal), transparency (citizens must know how their data is processed), and accountability (independent oversight and redress mechanisms) are crucial.⁵⁹ Constitutional morality in India, proportionality doctrines in Europe, and emerging AI ethics guidelines provide useful starting points for embedding these principles into governance.⁶⁰

Towards a Global Framework

The transition to the quantum era cannot be effectively governed through fragmented national responses alone. Post-quantum cryptography (PQC), artificial intelligence-assisted surveillance, transnational cybercrime, cloud-based data storage, and electronically authenticated evidence increasingly operate across territorial boundaries, whereas the legal safeguards regulating them remain predominantly domestic. This regulatory asymmetry creates an urgent need for an internationally coordinated framework capable of reconciling three interconnected objectives—cybersecurity, effective law enforcement, and protection of fundamental human rights. The Convention on Cybercrime, 2001 (Budapest Convention) represents an important starting point because it was designed to develop a common criminal policy against cybercrime through appropriate domestic legislation and enhanced international cooperation.⁶¹

The Budapest Convention was, however, formulated at a time when the present implications of quantum computing, generative artificial intelligence, large-scale biometric surveillance and quantum-resistant encryption were not part of mainstream legal discourse. Consequently, the quantum era may require what could conceptually be described as a next-generation international cyber-governance framework—not necessarily a replacement for the Budapest Convention, but an extension of its philosophy of international cooperation to address emerging cryptographic and surveillance technologies. Such a framework would need to regulate not merely cybercrime but also the standards governing quantum-secure communications, cross-border digital evidence, cryptographic authentication, algorithmic surveillance and protection of fundamental rights.

Thirdly, the convergence of AI-enabled surveillance with quantum-resilient infrastructure requires stronger transparency and accountability mechanisms. AI systems are already capable of identifying behavioural patterns, analysing biometric characteristics, processing large datasets and assisting public authorities in automated or semi-automated decision-making. PQC does not accelerate these functions; its role is to secure communications, authentication and data integrity against quantum-capable adversaries. Future quantum

computing may offer advantages for particular computational problems, including some optimisation or machine-learning tasks, but such advantage is application-dependent and should not be treated as a general acceleration of conventional AI surveillance. Governance should therefore regulate demonstrated surveillance capabilities while separately requiring appropriate cryptographic resilience.⁶²

A future quantum-era framework should, first, expressly incorporate the principles of legality, necessity and proportionality into the authorization and operation of technologically enhanced surveillance. The fact that quantum technologies may eventually make unprecedented levels of data processing, decryption or correlation technically possible does not mean that every technologically possible form of surveillance should become legally permissible. UNESCO's Recommendation on the Ethics of Artificial Intelligence adopts precisely this rights-oriented approach by providing that the use of AI systems should not go beyond what is necessary and proportionate to achieve a legitimate aim and that risk assessment should be employed to prevent possible harm⁶³. These principles should similarly form the normative foundation of quantum-enabled surveillance.

Secondly, a global framework should establish minimum standards for the authentication, preservation and cross-border admissibility of PQC-protected electronic evidence. Digital evidence collected in one country may be stored in another jurisdiction, transmitted through servers situated in several States, authenticated through cryptographic systems developed elsewhere, and ultimately presented before a court in a different country. The UN Convention against Cybercrime specifically recognizes the growing importance of international cooperation for collecting, preserving and sharing evidence in electronic form.⁶⁴ In the quantum context, this cooperative framework could eventually be supplemented by internationally accepted standards concerning PQC digital signatures, cryptographic metadata, chain of custody, algorithm migration, integrity verification and long-term preservation of digitally authenticated evidence.

Such harmonisation does not necessarily require the international community to impose a single cryptographic algorithm upon every State. Rather, the more appropriate objective would be to establish interoperability and mutual recognition standards capable of ensuring that electronic evidence authenticated through one approved quantum-resistant system remains legally and technically verifiable in another jurisdiction. Without such interoperability, differences in national cryptographic standards may themselves become obstacles to transnational investigation and administration of justice.

Thirdly, the convergence of artificial intelligence and quantum-enabled surveillance requires significantly stronger transparency and accountability mechanisms. AI systems are already capable of identifying behavioural patterns, analysing biometric characteristics, processing enormous datasets and assisting public authorities in automated or semi-automated decision-making. Quantum computing may substantially magnify these capacities by increasing computational speed and the ability to analyse complex datasets. UNESCO therefore treats transparency and explainability as essential conditions for protecting human rights and enabling individuals to challenge decisions based upon AI-generated outcomes.⁶⁵ It further recommends appropriate oversight, impact assessment, audit, due-diligence, traceability and accountability mechanisms throughout the lifecycle of AI systems.⁶⁶ Similar safeguards should become indispensable components of quantum-era surveillance governance.

The Global Digital Compact, adopted by the United Nations General Assembly in September 2024 as Annex I to the Pact for the Future, provides an even broader normative foundation for this emerging global architecture. The Compact recognizes both the transformative potential and the risks of emerging digital technologies and stresses that technological development must advance sustainable development and the full enjoyment of human rights. It specifically acknowledges the need to identify and mitigate technological risks and to ensure meaningful human oversight.⁶⁷

The Global Digital Compact is particularly relevant to quantum governance because it places privacy, data protection, accountability, interoperability and human rights within the international digital-governance agenda. It calls upon States to ensure that data is collected, accessed, shared, transferred, stored and processed in safe, secure and proportionate ways for explicit and legitimate purposes and in accordance with

international law.⁶⁸ These principles could provide the conceptual foundation for future international norms governing quantum-enabled processing and surveillance of personal data.

A further dimension requiring urgent attention is the danger of a global quantum divide. Migration to PQC will demand substantial financial resources, sophisticated digital infrastructure, specialised expertise, cryptographic inventories, secure hardware, institutional preparedness and sustained investment in research and development. Advanced technological economies may therefore complete the transition much earlier than developing and least-developed States. The Global Digital Compact expressly recognises that digital divides continue to exist both between and within countries and that these inequalities particularly affect developing countries with limited resources.⁶⁹ A global quantum-governance framework must therefore incorporate technical assistance, knowledge sharing, infrastructure support, research collaboration and institutional capacity-building rather than merely prescribing technological standards that poorer States may be unable to implement.

This issue assumes particular significance for the Global South. Quantum governance should not evolve exclusively through technological standards developed by a small group of technologically dominant States and corporations and thereafter transmitted to developing nations as predetermined norms. Such an arrangement could deepen technological dependency and reproduce what critical scholarship has described as forms of digital colonialism, where control over digital infrastructure, data, platforms and technological standards becomes concentrated in powerful foreign actors.⁷⁰ Meaningful participation by developing States in quantum standard-setting, cryptographic research, governance institutions and international negotiations is therefore necessary to ensure that quantum security becomes a genuinely global public good rather than another source of technological dependence.

The preceding analysis demonstrates that an ethically defensible framework for quantum-ready surveillance cannot be constructed through technological safeguards alone. Post-quantum cryptography may protect information against emerging computational threats, but cryptographic resilience does not determine whether information should be collected, how surveillance powers should be exercised, or what institutional safeguards should govern access to data. The framework developed here therefore consists of eight mutually reinforcing components: technological resilience and crypto-agility; constitutional legality; privacy and rights by design; accountable AI; institutional accountability; risk-tiered governance; global interoperability; and technological equity. These eight components are not separate checklists but stages and safeguards within the integrated governance cycle developed below.⁷¹

Regional organisations can serve as regulatory laboratories for developing these principles. Institutions such as the European Union and ASEAN may experiment with regional standards concerning privacy, digital identity, AI accountability, electronic evidence and cryptographic interoperability, while broader forums such as the United Nations and G20 can facilitate dialogue and convergence at the global level. A layered regulatory model may therefore be more realistic than immediate universal uniformity: minimum human-rights and cybersecurity safeguards could be established internationally; more detailed technical and regulatory standards could emerge regionally; and individual States could implement those standards through domestic legislation appropriate to their constitutional structures.

Ultimately, the central challenge is to ensure that a quantum-secure world does not become a quantum-surveilled world. The success of the transition to post-quantum cryptography cannot therefore be measured merely by the capacity of encryption systems to resist quantum attacks. It must also be assessed by whether the resulting technological architecture preserves privacy, human dignity, due process, equality, transparency and accountability. The emerging international framework should consequently move towards a model of “security by design, privacy by design and rights by design,” ensuring that the extraordinary capabilities of quantum technologies strengthen cybersecurity without simultaneously weakening the fundamental rights that cybersecurity is ultimately intended to protect.⁷²

Normative Blueprint for Ethical Quantum-Ready Surveillance

The preceding analysis demonstrates that an ethically defensible framework for quantum-ready surveillance cannot be constructed through technological safeguards alone. Post-quantum cryptography may protect information against emerging computational threats, but cryptographic resilience does not determine whether information should be collected, how surveillance powers should be exercised, or what institutional safeguards should govern access to data. A sustainable framework must therefore integrate technological resilience, constitutional legality, privacy-preserving design, accountable institutions, and international interoperability. In this sense, quantum readiness should be understood not merely as a cybersecurity objective, but as a broader model of responsible technological governance.

Technological Resilience: From PQC Adoption to Crypto-Agility

The first component must be technological resilience. The transition from quantum-vulnerable public-key cryptography to post-quantum cryptography has already moved from theoretical preparation to practical implementation. In August 2024, the U.S. National Institute of Standards and Technology finalized its first three principal post-quantum cryptographic standards—FIPS 203 for ML-KEM, FIPS 204 for ML-DSA and FIPS 205 for SLH-DSA—and encouraged organisations to begin migration rather than postpone transition until cryptographically relevant quantum computers become available.⁷³

Technological resilience, however, should not be reduced to a one-time replacement of RSA or elliptic-curve cryptography. The more sustainable objective is crypto-agility: information systems should be designed so that cryptographic algorithms, keys and protocols can be replaced without reconstructing the entire digital infrastructure. This is particularly important for governmental databases, critical infrastructure, financial networks, digital identity systems, judicial records and information requiring long-term confidentiality.

India's emerging policy direction reflects this approach. The Department of Science and Technology's 2026 Quantum Safe Ecosystem in India strategy envisages a phased transition towards quantum resilience, including cryptographic inventories, migration planning, hybrid deployment, testing and certification, crypto-agile public-key infrastructure and national testbeds.⁷⁴

The normative principle should therefore be:

Quantum security must be designed for continuous adaptability, not merely for the replacement of today's vulnerable algorithms.

Constitutional Legality: Technology Must Remain Subordinate to Law

The second component is constitutional legality. Quantum readiness cannot become an independent justification for expanding governmental surveillance powers. The acquisition of more powerful technological capability does not enlarge the constitutional authority of the State.

This distinction is particularly important in India after the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India. The nine-judge Constitution Bench held that privacy forms part of the constitutionally protected freedoms guaranteed under Part III and emphasized legality, legitimate State purpose and proportionality as essential considerations governing State interference with privacy.⁷⁵

Accordingly, quantum-enabled surveillance should satisfy a structured legal inquiry:

Is there clear legal authority? Is the objective legitimate? Is the measure necessary? Is the degree of intrusion proportionate? Are less intrusive alternatives reasonably available? Are safeguards and remedies adequate?

The normative architecture should therefore separate technological authorization from surveillance authorization. Administrative approval to install PQC-secured infrastructure, AI analytics or advanced computational systems should never be interpreted as implicit legal authority to collect additional information, expand interception, increase retention periods or undertake new forms of profiling.

Privacy and Rights by Design: Minimise Before Collecting

The third component should move beyond conventional privacy protection towards privacy-preserving system architecture. Regulation that intervenes only after excessive data has already been collected is inherently weaker than governance that minimizes unnecessary collection at the design stage.

The principle of privacy by design therefore requires surveillance systems to consider data minimisation, purpose limitation, pseudonymisation, controlled access, secure deletion and privacy-enhancing technologies before centralized collection becomes the default solution. UNESCO's global AI ethics framework similarly emphasizes privacy and data protection throughout the lifecycle of AI systems and links these safeguards to human dignity, autonomy and fundamental rights.⁷⁶

Where technically and operationally feasible, governments should therefore consider privacy-enhancing technologies such as federated analytics, secure multiparty computation, homomorphic encryption, differential privacy and controlled computation over encrypted or distributed datasets before constructing additional centralized repositories of personal information.

The normative presumption should be simple:

Collect only what is necessary; retain only for as long as justified; centralize only where decentralised or privacy-preserving alternatives cannot reasonably achieve the legitimate objective.

Accountable AI: Explainability Must Be Proportionate to Consequence

The fourth component concerns the growing convergence between AI and surveillance. Quantum computing and PQC should not be treated as synonymous with artificial intelligence; nevertheless, future surveillance architectures are likely to combine cryptographically secure infrastructure with AI-assisted identification, classification, anomaly detection, biometric analysis and predictive systems.

A blanket requirement that every AI model be completely explainable may be technically unrealistic. A more workable standard is consequence-sensitive explainability: the greater the impact of an automated output upon an individual's rights, liberty or legal position, the stronger the requirement for traceability, intelligible reasons, human review and contestability.

UNESCO identifies transparency and explainability, responsibility and accountability, and human oversight as important principles of responsible AI governance.⁷⁷ Thus, an algorithm that merely identifies network anomalies may require technical auditability; an AI system whose output contributes to identifying an individual as a security threat should attract substantially stronger safeguards, including meaningful human review.

Institutional Accountability: Every Exercise of Surveillance Power Must Leave an Audit Trail

The fifth component is institutional accountability. Rights cannot depend solely upon principles written into legislation; they require institutions capable of verifying compliance.

High-risk surveillance systems should therefore incorporate authorization records, access logs, purpose documentation, retention schedules, periodic audits and identifiable institutional responsibility. Oversight mechanisms—whether judicial, parliamentary, regulatory or independently administrative—should possess sufficient technical expertise to scrutinize sophisticated cryptographic and algorithmic systems.

The European Court of Human Rights' Grand Chamber has emphasized the importance of comprehensive safeguards throughout bulk-interception processes, including authorization, supervision and independent review,⁷⁸ Accountability should consequently be designed into the technological system itself. Every consequential access to protected surveillance information should answer four questions:

Who accessed the information? Under what authority? For what legally permissible purpose? For how long was the information retained or used?

A system incapable of answering these questions is difficult to reconcile with meaningful democratic oversight, regardless of the sophistication of its encryption.

Risk-Tiered Governance: Regulate According to Intrusiveness

The sixth component should be risk differentiation. Not every deployment of quantum-resistant cryptography or AI creates the same threat to fundamental rights. A government email system secured through PQC, an AI system detecting malware, facial recognition deployed in public spaces, and persistent biometric tracking of identified individuals raise fundamentally different legal concerns.

Governance should therefore classify surveillance technologies according to their intrusiveness, scale, sensitivity of data, degree of automation, duration, reversibility and consequences for individuals.

Low-risk applications may appropriately rely upon internal controls and routine auditing. Medium-risk applications may require formal impact assessment and independent periodic review. High-risk applications—particularly persistent biometric surveillance, bulk interception, cross-database profiling or systems capable of producing serious legal consequences—should attract enhanced authorization, necessity and proportionality review, strict retention limitations and effective avenues for redress.

Such differentiation avoids both regulatory extremes: under-regulating dangerous technologies and over-regulating beneficial security technologies.

Global Interoperability Without Regulatory Uniformity

The seventh component is international cooperation, but cooperation should not be confused with complete legal uniformity. States differ in constitutional traditions, security environments, institutional structures and levels of technological development. A realistic global framework should therefore establish minimum common safeguards and interoperable technical standards while preserving legitimate national flexibility.

The United Nations Global Digital Compact, adopted in 2024, provides an important normative foundation by emphasizing an inclusive, open, sustainable, fair, safe and secure digital future and by addressing privacy, responsible data governance, international cooperation, AI governance and capacity-building.⁷⁹

For the quantum environment, international convergence should initially concentrate upon practical areas where cooperation is achievable: recognition of approved PQC standards, cryptographic interoperability, authentication of electronic evidence, trusted timestamps, chain-of-custody requirements, incident reporting, vulnerability disclosure and migration of legacy systems.

The appropriate principle is therefore interoperability without imposed uniformity.

Technological Equity: Quantum Security Must Not Become a Privilege of Wealthy States

The eighth component is technological inclusion. Quantum-safe migration requires financial resources, specialized expertise, secure hardware, testing infrastructure and sustained institutional capacity. If only technologically advanced States can satisfy emerging quantum-security standards, the global transition could create a new security divide in which poorer States remain dependent upon technologies, vendors and standards developed elsewhere.

The Global Digital Compact recognizes persistent digital divides and places particular emphasis upon capacity-building and the participation of developing countries in digital governance.⁸⁰

International quantum governance should accordingly include technical assistance, open standards, shared testing infrastructure, training, research collaboration and affordable migration pathways for developing States. The participation of the Global South should extend beyond implementation; developing States should participate meaningfully in the formulation of standards themselves.

Otherwise, quantum security risks reproducing technological dependency rather than reducing it.

The Integrated Normative Model

These principles should not operate as isolated regulatory objectives. They form an integrated governance cycle:

Resilience → Legality → Necessity → Privacy by Design → Risk Classification → Authorization → Auditability → Independent Oversight → Redress → Periodic Review → International Interoperability.

The sequence is important. Technology asks what can be done; law determines what may be done; ethics asks what ought to be done; governance ensures that what is actually done remains accountable.

The normative objective of quantum-ready surveillance should therefore not be maximum surveillance secured by stronger cryptography, but minimum necessary surveillance protected by maximum appropriate security and accountable through effective institutions.

This distinction captures the central governance challenge of the quantum era. A technologically resilient surveillance system may still be constitutionally excessive; a legally authorized system may still be ethically disproportionate; and an ethically defensible national system may still fail if it cannot interact securely with international digital infrastructures. Responsible quantum governance must address all three dimensions simultaneously.

The quantum transition consequently represents more than a technological race. It is a test of whether legal institutions can develop at the same pace as technological power. If governance remains reactive, opaque and institutionally weak, quantum-ready infrastructure may magnify existing asymmetries of State and corporate power. If, however, resilience is combined with proportionality, privacy-preserving architecture, differentiated oversight, technical accountability and international inclusion, quantum technologies can strengthen security without requiring society to surrender the constitutional values that security exists to protect.

The Normative Proposition May Therefore Be Stated Succinctly:

A quantum-secure State should not be one in which the State can see everything and outsiders can see nothing; it should be one in which necessary information is securely protected, legitimate access is legally controlled, every intrusive exercise of power is accountable, and every individual remains protected by enforceable rights.

Yet stronger encryption does not automatically produce either greater surveillance capability or a more rights-respecting digital society. PQC secures confidentiality, authentication and integrity; it does not itself collect data, recognise faces, integrate databases or infer behaviour. Those surveillance capabilities arise from AI, biometrics, persistent sensing and large-scale data integration. The governance concern arises when such capability-expanding technologies operate inside increasingly secure, durable and interoperable infrastructures. The resulting system can become simultaneously more resistant to external compromise and more capable of sustaining intrusive internal monitoring. The normative question is therefore how

surveillance capability should be legally bounded while the infrastructure that supports it is made quantum-resilient.

CONCLUSION AND POLICY RECOMMENDATIONS

Concluding Remarks

The central argument emerging from this study is that the transition to a quantum-secure digital order is not merely a problem of replacing vulnerable cryptographic algorithms. It is a problem of institutional design, constitutional restraint, technological preparedness, and democratic accountability. Quantum computing exposes weaknesses in classical public-key cryptography, while post-quantum cryptography (PQC) offers an increasingly mature technical response. In August 2024, the U.S. National Institute of Standards and Technology (NIST) finalized its first three principal PQC standards—FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA)—and has since advised organisations to begin migration rather than wait for the arrival of a cryptographically relevant quantum computer.⁸¹ This development fundamentally changes the policy question: quantum readiness is no longer a distant theoretical concern; cryptographic migration has become a present governance responsibility.

Yet stronger encryption does not automatically produce a more rights-respecting digital society. The same technological ecosystem that enables governments to secure critical infrastructure, financial networks, defence communications and sensitive databases may also increase the scale, persistence and analytical power of surveillance. When PQC is combined with artificial intelligence, biometric identification, large-scale databases, predictive analytics and interoperable governmental information systems, the resulting infrastructure can become simultaneously more secure against external attack and more capable of internal monitoring. The normative question, therefore, is not whether the State should possess technologically advanced security capabilities. Modern States plainly require them. The more difficult question is how those capabilities should be legally bounded, institutionally supervised and technically designed so that security capacity does not become surveillance capacity without corresponding accountability.

The comparative analysis undertaken in this study demonstrates that there is no universal regulatory response. India, the United States and the European Union represent different legal traditions and institutional approaches to the relationship between privacy, security and governmental power. Their experience nevertheless reveals a common lesson: technological capability must be accompanied by legal authorization, purpose limitation, proportionality, institutional oversight and effective remedies. Privacy cannot depend solely upon the goodwill of the authority operating the technology; it must be embedded in the legal and technical architecture within which that authority operates.

This principle assumes particular significance in India. The National Quantum Mission, approved in 2023 with an outlay of ₹6,003.65 crore for 2023–24 to 2030–31, established a major national framework for quantum computing, communication, sensing and related technologies.⁸² More significantly for the present study, India's subsequent Quantum Safe Ecosystem in India strategy has moved the discussion from research to migration. The strategy envisages quantum resilience across Critical Information Infrastructure by 2029 and enterprise-wide adoption of PQC by 2033, together with testing and certification, hybrid deployment, crypto-agile public-key infrastructure and national testbeds.⁸³ CERT-In has likewise emphasized inventory, risk assessment and practical migration planning as components of quantum cyber-readiness.⁸⁴

These developments make the Indian policy debate particularly important. The task is no longer to decide whether India should prepare for quantum risk—it has already begun doing so—but to ensure that quantum-security policy and surveillance-governance policy evolve together rather than on separate tracks. A State may successfully migrate its cryptographic infrastructure and still fail to protect constitutional liberty if the resulting systems permit excessive collection, indefinite retention, opaque algorithmic profiling or inadequately supervised access to personal information.

At the international level, fragmentation remains an equally serious concern. Cryptographic systems are global, cloud infrastructures are transnational, electronic evidence routinely crosses borders, and cyber incidents rarely respect territorial jurisdiction. Yet rules governing surveillance authorization, data retention, evidentiary authentication, algorithmic accountability and remedies remain substantially national. The Global Digital Compact, adopted by the United Nations in 2024, provides an important normative direction by calling for responsible and interoperable data governance, privacy protection, proportionate processing, transparency, accountability and robust human oversight of AI systems.⁸⁵ The challenge now is to translate these principles into operational standards for the quantum era.

The deeper conclusion of this study is therefore that cryptographic strength and constitutional legitimacy are different forms of security, and a sustainable digital order requires both. PQC can protect a database against a future quantum attacker; it cannot determine whether the database should have been created, what information should have been collected, who should be permitted to access it, how long it should be retained, or what remedy should follow its misuse. Those remain questions for law, institutions and democratic governance.

Policy Recommendations: From Principle to Implementation

The appropriate policy response should therefore avoid two extremes: technological complacency on one side and indiscriminate surveillance expansion on the other. A workable framework should proceed through risk classification, phased migration, institutional accountability and measurable compliance rather than attempting to regulate every emerging technology through a single omnibus prohibition.

Establish a National Quantum-Security Governance Framework

India should establish a National Quantum Security Coordination Framework under the existing National Quantum Mission rather than immediately creating another independent bureaucracy. It should bring together DST, MeitY, CERT-In, NCIIPC, sectoral regulators, security agencies, standards bodies, data-protection institutions, technical experts and representatives of critical infrastructure.

Its function should be coordination rather than operational surveillance. It should issue common migration standards, identify priority sectors, prevent incompatible standards from emerging across departments, maintain national migration milestones, and periodically review quantum-security risks.

This approach is administratively viable because the institutional foundation already exists under the National Quantum Mission. India's 2026 Quantum Safe Ecosystem strategy itself envisages coordinated migration, testing, certification and crypto-agile infrastructure⁸⁶.

Make Cryptographic Inventory Mandatory Before Migration

Governments should resist the temptation to begin by purchasing new “quantum-safe” products. The first administrative requirement should be a Cryptographic Asset Inventory or Cryptographic Bill of Materials (CBOM).

Every ministry, critical-infrastructure operator, major financial institution, telecom operator and other designated entity should identify:

1. where RSA, ECC, Diffie–Hellman and other quantum-vulnerable algorithms are currently deployed;
2. what categories of information they protect;
3. how long that information must remain confidential;
4. which third-party vendors control relevant cryptographic dependencies; and
5. which systems cannot easily be upgraded.

This converts an abstract quantum threat into an auditable migration programme. CERT-In's technical

guidance already supports maintaining CBOM/QBOM information and adopting a risk-based quantum-readiness and migration strategy.⁸⁷

Adopt a Risk-Based Migration Schedule—Not a Single Deadline

PQC migration should be prioritized according to **risk and data lifespan**, rather than requiring every system to migrate simultaneously.

The first category should include defence, national-security communications, critical infrastructure, digital identity systems, financial infrastructure, health information and other data requiring long-term confidentiality. Lower-risk and short-lived information systems can follow later.

The policy should therefore use a simple administrative formula:

Priority = Sensitivity of Data × Required Confidentiality Period × Quantum Exposure × System Criticality.

This is more workable than an indiscriminate deadline because governments operate thousands of legacy systems with different technical and budgetary constraints. NIST similarly recommends identifying quantum-vulnerable systems and prioritizing migration, with its transition framework contemplating removal of quantum-vulnerable algorithms from standards by 2035 and earlier transition for high-risk systems.⁸⁸

Build “Crypto-Agility” into Every Major Government Procurement

The objective should not simply be to replace RSA or ECC once. Procurement standards should require crypto-agility—the ability to replace algorithms without redesigning the entire information system.

Future government tenders for cloud services, digital identity, financial systems, e-governance platforms, defence communications and critical infrastructure should therefore require vendors to disclose cryptographic dependencies, demonstrate migration capability, support approved PQC standards, provide algorithm-update mechanisms, and maintain backward-compatible transition plans.

Contracts should contain measurable migration milestones and vendor accountability provisions. This would convert quantum readiness from an advisory objective into an enforceable procurement condition and reduce future dependence on proprietary systems that cannot be economically upgraded.

Separate “Security Authorization” from “Surveillance Authorization”

One of the most important institutional safeguards should be the legal separation between authority to deploy secure technology and authority to use that technology for surveillance.

Approval of a PQC-enabled system should never itself authorize expanded collection, interception or profiling. High-risk surveillance should require a separate legal basis specifying purpose, categories of data, duration, access controls, retention limits and conditions for sharing.

Where the degree of intrusion is substantial, authorization should be subject to prior independent review appropriate to the constitutional and statutory framework. Emergency authorization may be permitted where genuinely necessary, but should be accompanied by documented reasons, strict duration limits and prompt post-facto review.

This distinction is essential because technological modernization should not silently expand governmental legal powers.

Introduce a Quantum-Surveillance Impact Assessment

Before deploying a high-risk surveillance system combining AI, biometrics, large-scale datasets or advanced cryptographic infrastructure, the responsible authority should complete a Quantum and Algorithmic Surveillance Impact Assessment (QASIA).

The assessment should answer practical questions: What legitimate objective is being pursued? Why are less intrusive alternatives inadequate? What categories of individuals may be affected? What data will be collected? How long will it be retained? Can an automated inference materially affect an individual? What human review exists? Who can audit the system? What happens if the system produces an erroneous result?

The assessment need not reveal operational secrets publicly. A classified version may be available to the competent oversight body, while a non-sensitive summary can be published. This reconciles legitimate secrecy with institutional accountability.

Create Tiered Oversight Rather Than Universal Prior Judicial Approval

Requiring a court order for every technologically assisted governmental activity would be administratively unrealistic. Oversight should instead correspond to the degree of intrusion.

Low-risk operations should require internal authorization and auditable logs. Medium-risk operations should require approval by a designated senior authority and periodic independent audit. High-risk surveillance—particularly interception, persistent biometric tracking, bulk collection or intrusive cross-database profiling—should attract enhanced independent or judicial authorization wherever required by the applicable constitutional and statutory framework.

This risk-tiered model concentrates scarce judicial and regulatory resources where the threat to individual rights is greatest.

Require Immutable Audit Trails and Individual Accountability

Every access to sensitive surveillance databases should generate a tamper-evident record identifying the authorized user, time, purpose, dataset accessed and action taken. High-risk systems should not permit anonymous institutional access.

Periodic automated review should identify unusual search patterns, excessive queries and unauthorized access. Where abuse occurs, responsibility should be traceable to identifiable officials rather than disappearing behind the abstraction of “the system.”

Accountability becomes effective only when the question “Who accessed this information, under whose authority, for what purpose, and for how long?” can be answered.

Preserve Evidentiary Reliability During Cryptographic Migration

PQC transition presents a neglected problem for courts: electronic records signed today may need to be proved decades later after the cryptographic algorithm originally used to authenticate them has been deprecated.

Governments should therefore establish a Long-Term Digital Evidence Preservation Protocol requiring preservation of original signatures and certificates, trusted timestamps, chain-of-custody metadata, migration records and, where necessary, periodic re-signing or re-timestamping using approved algorithms.

This is particularly important for land records, judicial records, governmental archives, intellectual-property records, financial instruments and evidence in long-running criminal or civil proceedings.

Use Privacy-Preserving Technologies Before Expanding Centralized Data Collection

Policy should create a privacy-preserving technology preference in public procurement. Before approving a centralized surveillance database, authorities should document whether the objective could reasonably be achieved through data minimisation, pseudonymisation, federated analytics, secure multiparty computation, homomorphic encryption or other privacy-enhancing techniques.

The governing principle should be straightforward:

Do not collect centrally what can reasonably be analysed securely without central collection.

This changes privacy from a restriction imposed after system design into an engineering requirement considered before deployment.

Establish Regulatory Sandboxes and Independent Testing

Government should not mandate immature quantum technologies across critical infrastructure without testing interoperability, performance, implementation security and operational continuity.

A national Quantum-Safe Regulatory Sandbox and Certification Programme should therefore permit banks, telecom operators, government departments and critical-infrastructure entities to test PQC deployment under controlled conditions before large-scale migration.

India's 2026 strategy already envisages national testing and certification mechanisms, hybrid deployment and testbeds for PQC and QKD solutions.⁸⁹

Build Capacity Before Creating Compliance Obligations

Quantum regulation without qualified personnel will produce paper compliance rather than security. India should establish specialized training streams for government IT officers, police cyber units, prosecutors, judges, forensic laboratories, regulators and auditors.

A national certification programme could create three levels—foundation, implementation and audit—allowing departments to build internal expertise instead of remaining permanently dependent upon external vendors.

Capacity-building should also extend internationally. The Global Digital Compact expressly calls for closing digital divides, developing skilled workforces and strengthening the capacity of developing countries to govern emerging technologies.⁹⁰

Pursue International Interoperability Before Attempting a New Global Treaty

An entirely new “Budapest Convention 2.0” may be normatively attractive but diplomatically difficult and institutionally slow. The immediate priority should therefore be interoperable technical and evidentiary standards, while treaty development remains a longer-term objective.

States can first cooperate on recognition of PQC signatures, minimum chain-of-custody requirements, cryptographic timestamping, incident reporting, common terminology, algorithm transition and cross-border electronic evidence. Existing institutions—including the United Nations, Council of Europe, ISO/IEC processes and regional organisations—can provide platforms for incremental convergence.

This staged approach is more workable than waiting for universal agreement before beginning cooperation.

Require Annual Quantum-Readiness Reporting

Finally, policy needs measurable outcomes. Designated government departments and critical-infrastructure

operators should submit an annual Quantum Readiness Statement containing at least:

1. percentage of cryptographic assets inventoried;
2. percentage of high-risk systems migrated;
3. number of legacy systems awaiting replacement;
4. vendor compliance status;
5. PQC interoperability tests completed;
6. significant implementation vulnerabilities identified;
7. personnel trained; and
8. projected budget and milestones for the following year.

A consolidated national report may publish non-sensitive indicators while security-sensitive details remain classified. What is measured can be administered; what is merely declared as policy is easily postponed.

Closing Observation

The quantum transition presents an unusual historical opportunity. Unlike many technological disruptions, society has received advance warning that widely used cryptographic systems will eventually need replacement. That warning creates not only an engineering opportunity but a governance responsibility.

The objective should therefore not be to construct the most powerful surveillance architecture that technology permits, nor to deny the State legitimate capabilities necessary to protect citizens and critical infrastructure. The more sustainable objective is to build a digital architecture in which security capability grows together with legal restraint, technical accountability and institutional oversight.

A quantum-secure system may protect information from an attacker. A rights-respecting legal order determines whether that information should have been collected in the first place. The first is the function of cryptography; the second is the function of constitutional governance. Neither can substitute for the other.

Accordingly, the central policy lesson of this study may be expressed in three propositions: migrate early, govern proportionately, and design for accountability. Cryptographic inventories, risk-based migration, crypto-agile procurement, independent oversight, privacy-preserving architecture, reliable digital-evidence standards, capacity-building and measurable annual reporting can translate those propositions from abstract principles into administrative practice.

The ultimate test of quantum readiness will therefore not be whether a State possesses the strongest encryption, the fastest computational capacity or the most sophisticated surveillance infrastructure. It will be whether that State can deploy technological power without allowing technological possibility to become legal inevitability.

Security and liberty need not stand at opposite ends of the quantum future. Properly governed, each can reinforce the other. The task for law and public policy is to ensure that the coming quantum architecture is not merely future-proof against machines, but institutionally trustworthy for human beings.

REFERENCE

1. Sr. Professor, Sant Gadge Baba Amravati University, Amravati. Any suggestions, criticism and critical appreciation may be reached at vijuchowbe@gmail.com. © authors.
2. Assistant Professor, Shri Rajasthani Seva Sangh Law College, Mumbai and Registered research Scholar at Research Centre (522), Dept of Law, SGB Amravati University Amravati with title “Contested terrain: A comparative analysis of policy framing, affirmative action, and legal protection for Scheduled Castes and Scheduled tribes in India.”
3. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, pp. 6–9. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

4. Buchanan, W., & Woodward, A. (2017). Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*, 1(1), 1-22. Retrieved from, <https://www.tandfonline.com/doi/abs/10.1080/23742917.2016.1226650> Visited on 12.02.2026
5. National Institute of Standards and Technology. (2024). What is post-quantum cryptography? U.S. Department of Commerce. Retrieved from, <https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography>. Visited on 26.05.2026.
6. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194.
7. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41.
8. Aldossary, S. M., & Kolhar, M. (2026). Quantum Sentinel Framework: Machine Learning-Based Detection and Mitigation of Quantum-Vulnerable Cryptography. Retrieved from, <https://assets-eu.researchsquare.com/files/rs-8777424/v1/f5794192-b482-470c-9b29-f6a88d8ac492.pdf> Visited on 14.05.2026
9. Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
10. Mantelero, A. (2022). AI and Human Rights: The balancing act. *Computer Law & Security Review*, 45, 105692.
11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
12. See, for more details, NIST selected CRYSTALS-Kyber and CRYSTALS-Dilithium for standardization in 2022; the final standards were issued on 13 August 2024 as FIPS 203 (ML-KEM, derived from Kyber), FIPS 204 (ML-DSA, derived from Dilithium) and FIPS 205 (SLH-DSA, derived from SPHINCS+)
13. Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. IEEE.
14. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41.
15. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194.
16. National Institute of Standards and Technology (NIST). (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST IR 8413. Kyber, Dilithium and SPHINCS+ were selected for standardization in 2022; final FIPS 203, 204 and 205 were published on 13 August 2024.
17. Lyon, D. (2022). *Surveillance Studies: An Overview*. Polity Press.
18. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
19. Creemers, R. (2022). China's social credit system: An evolving practice of control. *Information & Communications Technology Law*, 31(1), 1–20
20. Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
21. Casey, E. (2022). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.
22. Gunning, D., & Aha, D. (2021). DARPA's explainable AI (XAI) program. *AI Magazine*, 42(2), 56–65.
23. hang, Y., Wang, C., & Zhou, J. (2022). Blockchain forensics: Challenges and opportunities. *IEEE Transactions on Information Forensics and Security*, 17, 1265–1279.
24. European Commission. (2023). *Quantum Flagship: Building Europe's Quantum Future*. Brussels.
25. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. New Delhi.
26. NATO CCDCOE. (2023). *Locked Shields Cyber Defence Exercise: Annual Report*. Tallinn.
27. Mantelero, A. (2022). AI and human rights: The balancing act. *Computer Law & Security Review*, 45, 105692
28. Nye, J. (2022). *The Digital and Cybersecurity Challenge to National Security*. Harvard Kennedy School.
29. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
30. United Nations. (1966). *International Covenant on Civil and Political Rights*. UN Treaty Series, Vol. 999.

31. Electronic Frontier Foundation (EFF). (2021). FISA Section 702 and Mass Surveillance. San Francisco.
32. Government of India. (2023). Digital Personal Data Protection Act, 2023. New Delhi.
33. Creemers, R. (2022). China's cybersecurity regime. *Journal of Cyber Policy*, 7(1), 85–104
34. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
35. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights are violated by predictive policing systems. *NYU Law Review Online*, 94, 15–55.
36. Mantelero, A. (2022). AI and Human Rights: The balancing act. *Computer Law & Security Review*, 45, 105692.
37. Big Brother Watch and Others v. the United Kingdom [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013; [2021] ECHR 439.
38. Big Brother Watch and Others v. United Kingdom, ECHR, App Nos. 58170/13, 62322/14 and 24960/15 (2021).
39. Casey, E. (2022). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.
40. Bentham, J. (1789/2007). *An Introduction to the Principles of Morals and Legislation*. Dover Publications.
41. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights are violated by predictive policing systems. *NYU Law Review Online*, 94, 15–55.
42. United Nations General Assembly, 1948, Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217(III)
43. United Nations. (1948). Universal Declaration of Human Rights. UNGA Res. 217 A (III).
44. Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
45. Big Brother Watch and Others v. the United Kingdom [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013; [2021] ECHR 439.
46. Big Brother Watch and Others v. United Kingdom, ECHR, App Nos. 58170/13, 62322/14 and 24960/15 (2021).
47. Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1; AIR 2017 SC 4161.
48. Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
49. Bhandari, V., & Sinha, A. (2023). Data protection in India after DPDP Act: Promise and perils. *Indian Journal of Law and Technology*, 19(2), 67–94
50. Wheatley, M. C. (2024). Ethics of surveillance technologies: Balancing privacy and security in a digital age. *Premier Journal of Data Science*, 1, 100001. Retrieved from, https://www.researchgate.net/profile/Mary-Wheatley-2/publication/391641800_Ethics_of_Surveillance_Technologies_Balancing_Privacy_and_Security_in_a_Digital_Age/links/696cea50c906f117f2a6c0f0/Ethics-of-Surveillance-Technologies-Balancing-Privacy-and-Security-in-a-Digital-Age.pdf Visited on 11.09.2025
51. Ramanathan, U. (2020). Aadhaar: Governing with biometrics. *Seminar*, 734, 45–52.
52. Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.
53. Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.
54. Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
55. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 168, 24–31.
56. Nye, J. (2022). *The Digital and Cybersecurity Challenge to National Security*. Harvard Kennedy School.
57. Casey, E. (2022). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.
58. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.

59. Mantelero, A. (2022). AI and Human Rights: The balancing act. *Computer Law & Security Review*, 45, 105692.
60. Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
61. Council of Europe. (2001). Convention on Cybercrime, European Treaty Series No. 185, Budapest, 23 November 2001, Preamble, pp. 1–2. Council of Europe Treaty Office. See, <https://rm.coe.int/1680081561> Visited on 22.03.2026
62. United Nations General Assembly. (2024). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, G.A. Res. 79/243, U.N. Doc. A/RES/79/243, 24 December 2024, arts. 1, 35–40. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/243> Visited on 19.04.2026
63. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, adopted by the General Conference of UNESCO at its 41st Session, 23 November 2021, paras. 25–27, pp. 20–21. Paris: United Nations Educational, Scientific and Cultural Organization. Retrieved from, <https://unesdoc.unesco.org/ark:/48223/pf0000381137> Visited on 26.04.2026
64. United Nations General Assembly. (2024). United Nations Convention against Cybercrime, G.A. Res. 79/243, U.N. Doc. A/RES/79/243, 24 December 2024, Chapter V, arts. 35–40. Retrieved from, <https://docs.un.org/A/RES/79/243> Visited on 27.01.2026
65. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, paras. 37–41, pp. 22–23. Paris: UNESCO. Retrieved from, <https://unesdoc.unesco.org/ark:/48223/pf0000381137> Visited on 29.03.2026
66. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, paras. 42–43, pp. 23–24. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
67. United Nations General Assembly. (2024). Pact for the Future, Annex I: Global Digital Compact, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, adopted 22 September 2024, Annex I, paras. 1–7. United Nations, pp. 37–38. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 31.03.2026
68. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 37–40. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/1> visited on 21.08.2026.
69. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 2–3, 10–17. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 14.05.2026
70. Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, CA: Stanford University Press, pp. 1–22; See also, Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. Retrieved from, <https://doi.org/10.1177/0306396818823172> Visited on 01.02.2026
71. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 2, 10–17, 63–65. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 28.05.2026.
72. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, paras. 25–28, 32–43, pp. 20–24. See also, Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>; United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, Annex I. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 05.05.2026
73. National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204: Module-Lattice-Based Digital Signature Standard; FIPS 205: Stateless Hash-Based Digital Signature Standard, 13 August 2024. U.S. Department of Commerce. <https://csrc.nist.gov/projects/post-quantum-cryptography>
74. Department of Science and Technology, Government of India. (2026). Quantum Safe Ecosystem in India: Report of the Task Force on Post-Quantum Migration. National Quantum Mission, Government of India. <https://dst.gov.in/quantum-safe-ecosystem-in-india>

75. Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1; AIR 2017 SC 4161
76. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, adopted by the General Conference at its 41st Session, 23 November 2021, paras. 32–35, pp. 21–22. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
77. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, paras. 37–43, pp. 22–24. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
78. Big Brother Watch and Others v. the United Kingdom [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013; [2021] ECHR 439. Apps. Nos. 58170/13, 62322/14 & 24960/15, Judgment of 25 May 2021, ECHR 439, ECLI:CE:ECHR:2021:0525JUD005817013.
79. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, adopted 22 September 2024. United Nations. <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact>
80. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 10–17, 63–65. United Nations. <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact>
81. National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204: Module-Lattice-Based Digital Signature Standard; FIPS 205: Stateless Hash-Based Digital Signature Standard, 13 August 2024. U.S. Department of Commerce. Retrieved from, <https://csrc.nist.gov/projects/post-quantum-cryptography> Visited on 11.03.2026
82. Department of Science and Technology, Government of India. (2023). National Quantum Mission. Government of India. Retrieved from, <https://dst.gov.in/node/7223>. Visited on 26.03.2026
83. Department of Science and Technology, Government of India. (2026). Quantum Safe Ecosystem in India: Report of the Task Force on Post-Quantum Migration. National Quantum Mission, Department of Science and Technology. Retrieved from, <https://dst.gov.in/quantum-safe-ecosystem-in-india> Visited on 26.05.2026
84. Indian Computer Emergency Response Team (CERT-In) & SISA. (2025). Transitioning to Quantum Cyber Readiness. CERT-In, Government of India. Retrieved from, <https://www.cert-in.org.in/> Visited on 26.04.2026
85. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024. Retrieved from, <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact> Visited on 15.08.2025
86. Department of Science and Technology, Government of India. (2026). Quantum Safe Ecosystem in India: Report of the Task Force on Post-Quantum Migration. National Quantum Mission. Retrieved from, <https://dst.gov.in/quantum-safe-ecosystem-in-india> Visited on 15.05.2026.
87. See, Indian Computer Emergency Response Team (CERT-In). (2025). Technical Guidelines, Version 2.0, 9 July 2025, paras. 8.4.2.8–8.5.4, p. 51. Government of India. Retrieved from, <https://www.cert-in.org.in/> Visited on 20.04.2026
88. National Institute of Standards and Technology. (2024). NIST IR 8547: Transition to Post-Quantum Cryptography Standards, Initial Public Draft. U.S. Department of Commerce. Retrieved from, <https://doi.org/10.6028/NIST.IR.8547.ipd> Visited on 28.06.2026
89. Department of Science and Technology, Government of India. (2026). Quantum Safe Ecosystem in India. Retrieved from, <https://dst.gov.in/quantum-safe-ecosystem-in-india> Visited on 24.05.2026
90. United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024. Retrieved from, <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact> Visited on 30.04.2026

- 2 Assistant Professor, Shri Rajasthani Seva Sangh Law College, Mumbai and Registered research Scholar at Research Centre (522), Dept of Law, SGB Amravati University Amravati with title "Contested terrain : A comparative analysis of policy framing, affirmative action, and legal protection for Scheduled Castes and Scheduled tribes in India."
- 3 European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, pp. 6–9. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- 4 Buchanan, W., & Woodward, A. (2017). Will quantum computers be the end of public key encryption?. *Journal of Cyber Security Technology*, 1(1), 1-22. Retrieved from, <https://www.tandfonline.com/doi/abs/10.1080/23742917.2016.1226650> Visited on 12.02.2026
- 5 National Institute of Standards and Technology. (2024). What is post-quantum cryptography? U.S. Department of Commerce. Retrieved from, <https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography>. Visited on 26.05.2026.
- 6 Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194.
- 7 Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41.
- 8 Aldossary, S. M., & Kolhar, M. (2026). Quantum Sentinel Framework: Machine Learning-Based Detection and Mitigation of Quantum-Vulnerable Cryptography. Retrieved from, <https://assets-eu.researchsquare.com/files/rs-8777424/v1/f5794192-b482-470c-9b29-f6a88d8ac492.pdf> Visited on 14.05.2026
- 9 Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
- 10 Mantelero, A. (2022). AI and Human Rights: The balancing act. *Computer Law & Security Review*, 45, 105692.
- 11 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
- 12 See, for more details, NIST selected CRYSTALS-Kyber and CRYSTALS-Dilithium for standardization in 2022; the final standards were issued on 13 August 2024 as FIPS 203 (ML-KEM, derived from Kyber), FIPS 204 (ML-DSA, derived from Dilithium) and FIPS 205 (SLH-DSA, derived from SPHINCS+)
- 13 Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. IEEE.
- 14 Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41.
- 15 Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194.
- 16 National Institute of Standards and Technology (NIST). (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST IR 8413. Kyber, Dilithium and SPHINCS+ were selected for standardization in 2022; final FIPS 203, 204 and 205 were published on 13 August 2024.
- 17 Lyon, D. (2022). *Surveillance Studies: An Overview*. Polity Press.
- 18 Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- 19 Creemers, R. (2022). China's social credit system: An evolving practice of control. *Information & Communications Technology Law*, 31(1), 1–20
- 20 Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
- 21 Casey, E. (2022). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.
- 22 Gunning, D., & Aha, D. (2021). DARPA's explainable AI (XAI) program. *AI Magazine*, 42(2), 56–65.
- 23 hang, Y., Wang, C., & Zhou, J. (2022). Blockchain forensics: Challenges and opportunities. *IEEE Transactions on Information Forensics and Security*, 17, 1265–1279.
- 24 European Commission. (2023). *Quantum Flagship: Building Europe's Quantum Future*. Brussels.
- 25 Government of India. (2023). *Digital Personal Data Protection Act, 2023*. New Delhi.
- 26 NATO CCDCOE. (2023). *Locked Shields Cyber Defence Exercise: Annual Report*. Tallinn.
- 27 Mantelero, A. (2022). AI and human rights: The balancing act. *Computer Law & Security Review*, 45, 105692
- 28 Nye, J. (2022). *The Digital and Cybersecurity Challenge to National Security*. Harvard Kennedy School.
- 29 Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- 30 United Nations. (1966). *International Covenant on Civil and Political Rights*. UN Treaty Series, Vol. 999.
- 31 Electronic Frontier Foundation (EFF). (2021). *FISA Section 702 and Mass Surveillance*. San Francisco.
- 32 Government of India. (2023). *Digital Personal Data Protection Act, 2023*. New Delhi.
- 33 Creemers, R. (2022). China's cybersecurity regime. *Journal of Cyber Policy*, 7(1), 85–104
- 34 Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- 35 Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights are violated by predictive policing systems. *NYU Law Review Online*, 94, 15–55.
- 36 Mantelero, A. (2022). AI and Human Rights: The balancing act. *Computer Law & Security Review*, 45, 105692.

- 37 Big Brother Watch and Others v. the United Kingdom [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013; [2021] ECHR 439.
- 38 Big Brother Watch and Others v. United Kingdom, ECHR, App Nos. 58170/13, 62322/14 and 24960/15 (2021).
- 39 Casey, E. (2022). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.
- 40 Bentham, J. (1789/2007). *An Introduction to the Principles of Morals and Legislation*. Dover Publications.
- 41 Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights are violated by predictive policing systems. *NYU Law Review Online*, 94, 15–55.
- 42 United Nations General Assembly, 1948, Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217(III)
- 43 United Nations. (1948). Universal Declaration of Human Rights. UNGA Res. 217 A (III).
- 44 Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
- 45 Big Brother Watch and Others v. the United Kingdom [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013; [2021] ECHR 439.
- 46 Big Brother Watch and Others v. United Kingdom, ECHR, App Nos. 58170/13, 62322/14 and 24960/15 (2021).
- 47 Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1; AIR 2017 SC 4161.
- 48 Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
- 49 Bhandari, V., & Sinha, A. (2023). Data protection in India after DPDP Act: Promise and perils. *Indian Journal of Law and Technology*, 19(2), 67–94
- 50 Wheatley, M. C. (2024). Ethics of surveillance technologies: Balancing privacy and security in a digital age. *Premier Journal of Data Science*, 1, 100001. Retrieved from, https://www.researchgate.net/profile/Mary-Wheatley-2/publication/391641800_Ethics_of_Surveillance_Technologies_Balancing_Privacy_and_Security_in_a_Digital_Age/link/s/696cea50c906f117f2a6c0f0/Ethics-of-Surveillance-Technologies-Balancing-Privacy-and-Security-in-a-Digital-Age.pdf Visited on 11.09.2025
- 51 Ramanathan, U. (2020). Aadhaar: Governing with biometrics. *Seminar*, 734, 45–52.
- 52 Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.
- 53 Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.
- 54 Kuner, C. (2021). Transborder data flows and data privacy law. *Oxford Journal of Legal Studies*, 41(3), 530–557.
- 55 Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 168, 24–31.
- 56 Nye, J. (2022). *The Digital and Cybersecurity Challenge to National Security*. Harvard Kennedy School.
- 57 Casey, E. (2022). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.
- 58 Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- 59 Mantelero, A. (2022). AI and Human Rights: The balancing act. *Computer Law & Security Review*, 45, 105692.
- 60 Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
- 61 Council of Europe. (2001). *Convention on Cybercrime*, European Treaty Series No. 185, Budapest, 23 November 2001, Preamble, pp. 1–2. Council of Europe Treaty Office. See, <https://rm.coe.int/1680081561> Visited on 22.03.2026
- 62 United Nations General Assembly. (2024). *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, G.A. Res. 79/243, U.N. Doc. A/RES/79/243, 24 December 2024, arts. 1, 35–40. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/243> Visited on 19.04.2026
- 63 UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*, adopted by the General Conference of UNESCO at its 41st Session, 23 November 2021, paras. 25–27, pp. 20–21. Paris: United Nations Educational, Scientific and Cultural Organization. Retrieved from, <https://unesdoc.unesco.org/ark:/48223/pf0000381137> Visited on 26.04.2026
- 64 United Nations General Assembly. (2024). *United Nations Convention against Cybercrime*, G.A. Res. 79/243, U.N. Doc. A/RES/79/243, 24 December 2024, Chapter V, arts. 35–40. Retrieved from, <https://docs.un.org/A/RES/79/243> Visited on 27.01.2026
- 65 UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*, paras. 37–41, pp. 22–23. Paris: UNESCO. Retrieved from, <https://unesdoc.unesco.org/ark:/48223/pf0000381137> Visited on 29.03.2026
- 66 UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*, paras. 42–43, pp. 23–24. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

- 67 United Nations General Assembly. (2024). Pact for the Future, Annex I: Global Digital Compact, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, adopted 22 September 2024, Annex I, paras. 1–7. United Nations, pp. 37–38. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 31.03.2026
- 68 [United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 37–40. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/1> visited on 21.08.2026.
- 69 United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 2–3, 10–17. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 14.05.2026
- 70 Couldry, N., & Mejias, U. A. (2019). The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford, CA: Stanford University Press, pp. 1–22; See also, Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. Retrieved from, <https://doi.org/10.1177/0306396818823172> Visited on 01.02.2026
- 71 United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 2, 10–17, 63–65. United Nations. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 28.05.2026.
- 72 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, paras. 25–28, 32–43, pp. 20–24. See also, Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>; United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, Annex I. Retrieved from, <https://docs.un.org/A/RES/79/1> Visited on 05.05.2026
- 73 National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204: Module-Lattice-Based Digital Signature Standard; FIPS 205: Stateless Hash-Based Digital Signature Standard, 13 August 2024. U.S. Department of Commerce. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- 74 Department of Science and Technology, Government of India. (2026). Quantum Safe Ecosystem in India: Report of the Task Force on Post-Quantum Migration. National Quantum Mission, Government of India. <https://dst.gov.in/quantum-safe-ecosystem-in-india>
- 75 Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1; AIR 2017 SC 4161
- 76 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, adopted by the General Conference at its 41st Session, 23 November 2021, paras. 32–35, pp. 21–22. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- 77 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, paras. 37–43, pp. 22–24. Paris: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- 78 Big Brother Watch and Others v. the United Kingdom [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, Judgment of 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013; [2021] ECHR 439. Apps. Nos. 58170/13, 62322/14 & 24960/15, Judgment of 25 May 2021,⁷⁸ ECHR 439, ECLI:CE:ECHR:2021:0525JUD005817013].
- 79 United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, adopted 22 September 2024. United Nations. <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact>
- 80 United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024, paras. 10–17, 63–65. United Nations. <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact>
- 81 National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204: Module-Lattice-Based Digital Signature Standard; FIPS 205: Stateless Hash-Based Digital Signature Standard, 13 August 2024. U.S. Department of Commerce. Retrieved from, <https://csrc.nist.gov/projects/post-quantum-cryptography> Visited on 11.03.2026
- 82 Department of Science and Technology, Government of India. (2023). National Quantum Mission. Government of India. Retrieved from, <https://dst.gov.in/node/7223>. Visited on 26.03.2026
- 83 Department of Science and Technology, Government of India. (2026). *Quantum Safe Ecosystem in India: Report of the Task Force on Post-Quantum Migration*. National Quantum Mission, Department of Science and Technology. Retrieved from, <https://dst.gov.in/quantum-safe-ecosystem-in-india> Visited on 26.05.2026
- 84 [Indian Computer Emergency Response Team (CERT-In) & SISA. (2025). Transitioning to Quantum Cyber Readiness. CERT-In, Government of India. Retrieved from, <https://www.cert-in.org.in/> Visited on 26.04.2026
- 85 United Nations General Assembly. (2024). *Global Digital Compact, Annex I to Pact for the Future*, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024. Retrieved from, <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact> Visited on 15.08.2025

- ⁸⁶Department of Science and Technology, Government of India. (2026). Quantum Safe Ecosystem in India: Report of the Task Force on Post-Quantum Migration. National Quantum Mission. Retrieved from, <https://dst.gov.in/quantum-safe-ecosystem-in-india> Visited on 15.05.2026.
- ⁸⁷ See, Indian Computer Emergency Response Team (CERT-In). (2025). Technical Guidelines, Version 2.0, 9 July 2025, paras. 8.4.2.8–8.5.4, p. 51. Government of India. Retrieved from, <https://www.cert-in.org.in/> Visited on 20.04.2026
- ⁸⁸ National Institute of Standards and Technology. (2024). *NIST IR 8547: Transition to Post-Quantum Cryptography Standards*, Initial Public Draft. U.S. Department of Commerce. Retrieved from, <https://doi.org/10.6028/NIST.IR.8547.ipd> Visited on 28.06.2026
- ⁸⁹ Department of Science and Technology, Government of India. (2026). *Quantum Safe Ecosystem in India*. Retrieved from, <https://dst.gov.in/quantum-safe-ecosystem-in-india> Visited on 24.05.2026
- ⁹⁰ United Nations General Assembly. (2024). Global Digital Compact, Annex I to Pact for the Future, G.A. Res. 79/1, U.N. Doc. A/RES/79/1, 22 September 2024. Retrieved from, <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact> Visited on 30.04.2026