QUANTUM TECHNOLOGIES AND HUMAN RIGHTS UNDER INTERNATIONAL LAW

Islombek Abdikhakimov
Lecturer of Cyber Law Department
islombekabduhakimov@gmail.com

Abstract: *Quantum technologies, including computing, sensing, and communications, promise transformative advances in fields such as medicine, cryptography, and materials science, yet they also pose profound challenges to human rights under international law. The capacity of quantum computers to break widely used public-key encryption threatens the right to privacy and data protection, enabling mass surveillance and chilling effects on freedom of expression, while enhanced quantum sensing amplifies state and non-state surveillance capabilities. Conversely, these technologies can support the right to enjoy the benefits of scientific progress by accelerating research and innovation, provided equitable access is ensured to avoid exacerbating global inequalities. As of November 2025, international human rights law—primarily through instruments like the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the European Convention on Human Rights (ECHR)—provides a framework for addressing these dualities, imposing obligations on states to protect rights from third-party interference and to foster scientific freedom responsibly. However, governance remains fragmented, with no dedicated treaties and reliance on soft-law initiatives from UNESCO, the UN, and OECD. This article analyzes key human rights implications, current legal gaps, and pathways toward rights-compatible governance, arguing for proactive multilateral norms to ensure quantum advances uphold dignity, privacy, and equity.*

Kalit so‘zlar: *quantum technologies, human rights, international law, right to privacy, freedom of expression, right to science, encryption, surveillance, digital divide, governance frameworks*

The advent of the **second quantum revolution**, driven by the precise manipulation of fundamental quantum phenomena such as superposition, entanglement, and tunneling, is fundamentally reshaping computational paradigms and sensory precision in ways that classical technologies cannot match. This transformative shift is underpinned by massive global investment, with consolidated public and private expenditures surpassing tens of billions of dollars annually. Major economies, including **China** (with its multi-billion dollar national laboratory), the **United States** (through its National Quantum Initiative), the **European Union** (via the Quantum Flagship), and increasingly significant commitments from emerging players like **India**, **Australia**, and the **UK**, are locked in a strategic race for quantum supremacy.

This revolution rests on three core pillars. **Quantum computing** harnesses indeterminate qubit states to perform parallel computations, offering exponential speed-ups for specific algorithms. **Quantum sensing** leverages the exquisite sensitivity of quantum states to achieve measurement precision orders of magnitude beyond any classical limit. Finally, **quantum communications** leverage principles like the no-cloning theorem for information-theoretic security. These capabilities, while nascent, are rapidly transitioning from controlled laboratory experiments to practical, real-world deployments. This is evidenced by China's pioneering *Micius* satellite, which established intercontinental quantum-secured communication, and the ambitious technology roadmaps of private firms like IBM and Google, which aim for fault-tolerant quantum systems by the early 2030s.

This technological frontier intersects directly with the established corpus of **international human rights law (IHRL)**. This legal framework—rooted in the Universal Declaration of Human Rights (UDHR) and codified in binding treaties like the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and regional instruments like the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights—is not silent on emerging technologies. It mandates a robust, **tripartite typology of state obligations: to respect, protect, and fulfill** human rights. States must *respect* rights by abstaining from quantum-enabled violations (e.g., mass surveillance). They must *protect* rights by safeguarding individuals against third-party harms, including those from powerful corporations developing quantum systems. And they must *fulfill* rights by proactively enabling rights enjoyment, which includes ensuring equitable access to quantum's benefits and fostering international cooperation under Article 2(1) of the ICESCR, an obligation that increasingly carries extraterritorial implications in a globally networked world.

The pronounced **dual-use character** of quantum systems, where civilian breakthroughs in materials science or medicine can be rapidly repurposed for military or repressive ends, necessitates foresightful, adaptive regulation. This regulation must

balance the imperative for scientific freedom (enshrined in Article 15(3) ICESCR) with the urgent need for risk mitigation. As the Committee on Economic, Social and Cultural Rights (CESCR) articulated in its **General Comment No. 25**, which explicitly addresses the digital environment, states' obligations extend fully to this new domain, and it calls for proactive measures such as mandatory human rights impact assessments (HRIAs) *before* technologies are deployed.

A core and immediate threat emanates from quantum computing's unparalleled **cryptanalytic prowess**. Specifically, Peter Shor's 1994 algorithm provides a method for quantum computers to efficiently factor large prime numbers and solve discrete logarithm problems. This capability renders obsolete the cryptographic protocols—primarily **RSA, ECC, and Diffie-Hellman**—that secure the vast majority of global digital infrastructure. Everything from online banking and e-commerce (SSL/TLS) to secure government communications, digital signatures, and blockchain technologies is rendered vulnerable.

Intelligence agencies are widely believed to be engaging in **"Harvest now, decrypt later" (HNDL)** strategies. This involves intercepting and storing massive volumes of currently encrypted data, which is cheap and easy to do, with the expectation of decrypting it retroactively once a sufficiently powerful quantum computer becomes available. The implications for human rights are profound. Decades of data—including the privileged communications of journalists and their sources, sensitive medical records, classified state information, and the private correspondence of activists and dissidents—could be unlocked, creating a retrospective panopticon. This directly implicates the **right to privacy (Article 17 ICCPR)**.

The UN High Commissioner for Human Rights has explicitly warned that surveillance capabilities enabling such bulk interception are fundamentally incompatible with the stringent **necessity and proportionality tests** required under IHRL. This interpretation has been robustly affirmed by tribunals like the European Court of Human Rights (ECtHR) in cases such as *Szabó and Vissy v. Hungary* and *Zakharov v. Russia*, where bulk interception regimes were deemed unlawful precisely because they lacked targeted safeguards and effective oversight. Furthermore, as the Court of Justice of the European Union (CJEU) affirmed in the *Schrems II* decision, the mere *potential* for such bulk access by foreign intelligence can invalidate international data transfer mechanisms, highlighting the gravity of the threat. Beyond direct privacy violations, the anticipated power of quantum decryption casts a severe **chilling effect** on freedom of expression (Article 19 ICCPR), as individuals, fearing future exposure, may self-censor their communications, associations, and online activities.

This threat profile triggers strong positive obligations for states. They must mandate and fund a rapid, orderly **migration to post-quantum cryptography (PQC)**—new cryptographic standards believed to be secure against both classical and quantum attacks. The **US National Institute of Standards and Technology (NIST)** has been

leading this global effort since 2016, culminating in the 2022 selection of initial standardized algorithms like CRYSTALS-Kyber. States must also legislate to prohibit the private development or sale of quantum decryption tools without rigorous democratic oversight, while carefully tailoring export controls to avoid unduly restricting legitimate scientific research.

The threats are not limited to computing. **Quantum sensing technologies**—including ultra-precise magnetometry, gravimetry, and atomic clocks—enable detection modalities that are radically more powerful than their classical counterparts. These sensors can "see" through barriers (e.g., "quantum radar"), detect subterranean structures, or identify individuals from a distance via unique biometric signatures like their heartbeat or neural activity. This non-invasive, remote surveillance potential drastically amplifies the power of both state intelligence agencies and corporate data brokers.

When integrated with **AI-driven analytics**, particularly quantum machine learning (QML) which could accelerate pattern recognition, these tools pose an existential risk to anonymity. They could facilitate ubiquitous **predictive policing** systems or enhance dystopian **social credit systems**, risking profoundly discriminatory outcomes. Such systems, often trained on biased data, are likely to disproportionately target marginalized communities, constituting a clear violation of the non-discrimination clauses in **Article 26 ICCPR** and **Article 14 ECHR**.

The **UN Special Rapporteur on freedom of opinion and expression** has also flagged the threat of quantum-enhanced disinformation. Quantum optimization algorithms could potentially generate hyper-realistic **deepfakes** at unprecedented scale and speed, or micro-target persuasive propaganda far more effectively than current AI. This capability could fatally undermine democratic discourse, pollute the information ecosystem, and sabotage the right to seek and receive information under **Article 19 UDHR**. Furthermore, rights to **assembly and association (Articles 21-22 ICCPR)** are directly jeopardized when quantum imaging or sensing technologies can track protestors through dense urban environments, identify them through walls, or monitor concealed meetings, effectively eliminating "practical obscurity" as a safeguard for civil society.

Addressing these threats requires that any deployment be subject to the strictest tests of necessity and proportionality, including prior, independent judicial warrants. Principles of **data minimization** and **transparency** are paramount. However, the inherent **"black-box" nature** of many complex quantum algorithms, similar to AI, severely complicates accountability and oversight. It is difficult for a court or oversight body to assess the proportionality of a system whose decision-making logic is probabilistic and computationally irreducible. This challenge necessitates new accountability paradigms, such as the mandatory algorithmic impact assessments and auditability requirements proposed under mechanisms like the **EU AI Act**, and reinforces the need for an enforceable right to an effective remedy (Article 13 ICCPR).

Conversely, quantum technologies are not merely a source of risk; they are a profound embodiment of the **Right to Enjoy the Benefits of Scientific Progress and its Applications (REBSPA)**, as enshrined in **Article 27 UDHR** and **Article 15(1)(b) ICESCR**. Quantum systems promise to accelerate solutions to humanity's most pressing challenges. In **precision medicine**, quantum computers could simulate complex molecular and protein interactions, revolutionizing drug design and personalized treatments for diseases like cancer and Alzheimer's. In **climate science**, they could model complex weather systems with new fidelity, predicting natural disasters or optimizing the development of new carbon-capture materials. Their optimization capabilities could also unlock new efficiencies in energy grids, logistics, and finance, directly contributing to the **Sustainable Development Goals (SDGs)**.

The **CESCR's General Comment No. 25** elucidates the core state obligations under REBSPA: ensuring fair and equitable *access* to these applications, fostering *participation* in the scientific enterprise, and *protecting* scientific freedoms. The **Venice Statement (2009)** further emphasizes the critical importance of international **benefit-sharing**. Indeed, quantum technology itself offers privacy-enhancing solutions. **Quantum Key Distribution (QKD)**, for example, offers provably secure communication channels based on the laws of physics, providing a potential lifeline for human rights defenders, journalists, and minorities operating in repressive regimes.

However, equitable distribution is imperative. A widening **"quantum divide"**—whereby wealthy nations and corporations monopolize quantum capabilities—risks creating a new axis of global inequality. Such a divide would entrench existing economic and social disparities, violating the fundamental principle of **non-discrimination (Article 2(2) ICESCR)**, as developing states are left without the infrastructure, financial resources, or specialized talent to participate. This is not just a development issue; it is a rights imperative. The obligation for **international cooperation and assistance (Article 15(4) ICESCR)** becomes a central legal duty, mandating technology transfer, open-source initiatives, and global capacity-building, as urged by **UNESCO's ROAM framework** (Rights-based, Open, Accessible, Multi-stakeholder).

Despite the high stakes, **governance under international law is presently fragmented and inadequate**, comprised almost entirely of non-binding soft-law principles rather than enforceable hard-law instruments. **UNESCO's 2024 report** on the ethics of quantum technology advocates for a human rights-centered governance model, proposing ten key principles including the prohibition of rights-violating applications and a commitment to fairness in access. Similarly, the **World Economic Forum's 2022 Quantum Computing Governance Principles** call for transparency, responsible development, and inclusive dialogue. Security-focused bodies like **UNIDIR** (UN Institute for Disarmament Research) and the new **UN Scientific Advisory Board** have begun to highlight the profound risks to international peace and security, which intersect

directly with human rights.

While these initiatives are valuable, they lack enforcement. National strategies, such as the **US National Quantum Initiative** and the **EU Quantum Flagship**, incorporate ethical guidelines ("ethics-by-design"), but these are often vague and lack the legal force to constrain national security or corporate interests. In the absence of a binding treaty, **standardization bodies** like the **ISO** and **ITU** become crucial, yet highly-politicized, proxy arenas for normative influence. This creates a significant risk of **authoritarian capture**, where states with repressive models of governance attempt to embed surveillance-friendly protocols into the very technical architecture of the quantum internet, normalizing rights violations at the level of code.

Implementation challenges for a rights-based approach abound. Tensions immediately arise between **scientific freedom** and **precautionary controls**. Overly broad export control regimes, such as the **Wassenaar Arrangement** which governs dual-use technologies, could stifle the very international academic collaboration needed for scientific progress, yet weak controls risk proliferation. A second major challenge is the **opacity of private-sector R&D**. A significant portion of cutting-edge research occurs within corporations like Google, Microsoft, and IBM, shielded by commercial secrecy. This opacity hinders public oversight and the effective implementation of human rights due diligence, as articulated in the **UN Guiding Principles on Business and Human Rights (UNGPs)**.

Furthermore, traditional IHRL is state-centric, yet powerful **non-state actors**—from corporations to sophisticated criminal syndicates—may be the first to develop or acquire quantum capabilities, evading direct state obligations. The sheer **foreseeability of these harms**, even if their timeline is uncertain, triggers the need for precautionary approaches without halting progress, a delicate balance outlined in CESCR guidance. This balance is further threatened by the **geopolitical race** for quantum advantage, which incentivizes secrecy, discourages data sharing, and undermines the transparency rights essential for democratic accountability.

To navigate this complex landscape, several **recommendations** are proposed. First, states should begin negotiations toward a **UN framework convention on quantum governance**, similar to the "convention-protocol" model used for climate change (UNFCCC). This treaty would establish core principles, including mandatory, independent **human rights impact assessments** for all large-scale quantum projects. Second, a hard deadline, such as **2030**, should be mandated for public-sector migration to **NIST-approved PQC standards** to mitigate the HNDL threat. Third, **inclusive international observatories** must be established to monitor quantum developments, ensuring participation from scientists, ethicists, and civil society from the Global South, not just the "quantum powers."

Fourth, **public-private partnerships** must be reoriented toward equitable access

and open-source models, preventing the monopolization of benefits. Fifth, the **REBSPA** must be integrated as a core, rather than peripheral, element in all quantum development agendas, linking scientific progress explicitly to human empowerment. Finally, **civil society** and the technical community must be actively engaged and funded to counter the inherent power imbalances in discussions dominated by state security and corporate interests. A proposed set of binding principles—**prohibiting** inherently harmful uses (e.g., autonomous quantum weapons), ensuring **proportionality** and oversight for dual-use applications, promoting **benefit-sharing**, and requiring **transparency**—could form the normative basis for such a treaty.

In conclusion, the quantum technology revolution constitutes a profound **stress-test for international human rights law's adaptability** in the 21st century. The challenge is both technical and normative. By embedding **rights-by-design** from the very inception of R&D—not as an afterthought but as a core design principle—the global community can navigate this transition. Through mandatory impact assessments, robustly inclusive governance, and precautionary regulation, the quantum era can fulfill the promise of REBSPA, resulting in shared progress and enhanced human capabilities. Failure to act decisively risks a dystopian landscape of pervasive control, unbreakable surveillance, and entrenched inequality. Proactive, rights-based multilateralism offers the only viable path toward a future of empowerment and dignity.

REFERENCES

van Daalen, O. (2024). Developing a human rights compatible governance framework for quantum computing. *Research Directions: Quantum Technologies*, 2, e1. https://doi.org/10.1017/qut.2024.1

Krishnamurthy, V. (2025). Human rights and democracy in the quantum age. *Just Security*. https://www.justsecurity.org/108168/quantum-age/

Kop, M. (2021). Establishing a legal-ethical framework for quantum technology. *Yale Journal of Law & Technology*. https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology

UNESCO. (2024). *Human rights centered global governance of quantum technologies*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000393402

World Economic Forum. (2022). *Quantum computing governance principles*. https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf

Vermaas, P., & Mans, U. (2024). *Quantum technologies and their global impact: Discussion paper*. Quantum Delta NL for UNESCO. https://assets.quantum-delta.prod.verveagency.com/assets/quantum-technologies-and-their-global-impact:-discussion-paper.pdf

Committee on Economic, Social and Cultural Rights. (2020). General Comment No. 25 on science and economic, social and cultural rights. UN Doc. E/C.12/GC/25.

United Nations Institute for Disarmament Research. (2024). Quantum technologies and their implications for international peace and security (Programme). https://unidir.org/wp-content/uploads/2024/11/ID24programme_Final.pdf

Krishnamurthy, V. (2022). Quantum technology and human rights: An agenda for collaboration. *Quantum Science and Technology*, 7(4), 044003.

Quantum Delta NL. (2024). *Quantum technologies and their global impact*. https://assets.quantum-delta.prod.verveagency.com/assets/quantum-technologies-and-their-global-impact:-discussion-paper.pdf

Hoffmann, C. H., & Flöther, F. F. (2024). Why business adoption of quantum and AI technology must be ethical. *Research Directions: Quantum Technologies*.

United Nations Scientific Advisory Board. (2025). *Quantum computing*. United Nations. https://www.un.org/scientific-advisory-board/sites/default/files/2025-06/quantum_computing.pdf

Malekos Smith, Z. L., et al. (2024). Quantum technology, peace and security: A primer. United Nations Institute for Disarmament Research. https://unidir.org/wp-content/uploads/2024/11/UNIDIR_quantum_technology.pdf