Science
Conference

Vol.4 N.1 (2026)
science-conference.com

RETROACTIVE DECRYPTION AND THE RIGHT TO PRIVACY: EVALUATING STATE DUE DILIGENCE IN THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

Islombek Abdikhakimov
islombekabduhakimov@gmail.com

ABSTRACT

The imminent arrival of Cryptographically Relevant Quantum Computers (CRQCs) threatens to dismantle the cryptographic foundations of global privacy rights through the "Harvest Now, Decrypt Later" (HNDL) strategy. This adversarial practice, wherein encrypted data is intercepted today for future decryption, creates a "privacy time-bomb" that challenges the temporal scope of human rights obligations. This article evaluates the compatibility of the "Harvest Now, Decrypt Later" threat with the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). It examines whether the state's failure to mandate Post-Quantum Cryptography (PQC) constitutes a breach of the due diligence obligation to protect the right to privacy. Through a doctrinal analysis of international jurisprudence and technical readiness assessments, the study finds that the current "wait-and-see" regulatory approach effectively tolerates the retroactive violation of privacy. The article concludes that the international legal principle of due diligence must be reinterpreted to include a "crypto-agility mandate," compelling states to transition critical infrastructure to quantum-safe standards immediately to prevent a future where privacy is rendered technologically impossible.

KEYWORDS

Retroactive Decryption, Right to Privacy, HNDL, Post-Quantum Cryptography, Due Diligence, State Responsibility, Human Rights.

INTRODUCTION

Introduction

The digital age has tethered the realization of the right to privacy to the strength of cryptographic protocols. For decades, public-key encryption schemes such as RSA and Elliptic Curve Cryptography (ECC) have served as the technical guarantor of privacy for private communications, medical records, and financial transactions. However, the rapid advancement of quantum computing threatens to shatter this shield. As detailed in recent technical literature, future Cryptographically Relevant Quantum Computers (CRQCs) will possess the ability to run Shor's algorithm, efficiently factoring large integers and solving discrete logarithm problems that underpin current encryption standards (Erol, 2025). This capability gives rise to the "Harvest Now, Decrypt Later" (HNDL) threat model, where adversaries collect encrypted data today with the intent of decrypting it once quantum technology matures (Jena, 2025).

The legal implications of HNDL are profound and unprecedented. Unlike traditional data breaches where the harm is immediate and visible, HNDL represents a deferred injury. The violation of privacy is set in motion at the moment of interception ("harvesting"), but the actual exposure of the private information ("decryption") may occur years later. This temporal decoupling creates a significant challenge for human rights law, which typically adjudicates violations based on present harm or imminent threat. The core legal question is whether the state's positive obligation to protect the right to privacy extends to preventing future, retroactive violations caused by the obsolescence of current technological standards.

International human rights law, specifically Article 17 of the ICCPR and Article 8 of the ECHR, imposes a positive obligation on states to ensure respect for private life. This obligation includes protecting individuals from unlawful interference by third parties, including foreign state actors and cybercriminals. In the context of cyberspace, this duty has been interpreted to require "due diligence"—the taking of reasonable measures to prevent foreseeable harm (Kastelic, 2019). The HNDL threat is now a foreseeable risk, acknowledged by

major intelligence agencies and technical bodies like NIST (Erol, 2025). Consequently, the continued reliance on classical encryption in critical infrastructure may no longer satisfy the standard of due diligence required by international law.

The "quantum reckoning" forces a re-evaluation of the "reasonable expectation of privacy." If the encryption protecting a citizen's data is known to be vulnerable to a future attack, does the citizen still possess a reasonable expectation that their data will remain private? Courts have historically ruled that individuals assume the risk of disclosure when sharing data with third parties (Cohen et al., 2016). However, in a digital society where participation requires the use of encrypted channels, the "assumption of risk" doctrine may be ill-suited to address systemic vulnerabilities that individuals cannot mitigate on their own. The state, as the regulator of digital infrastructure, bears the primary responsibility for ensuring that the technological environment is conducive to the exercise of rights.

This article posits that the transition to Post-Quantum Cryptography (PQC) is not merely a technical upgrade but a human rights imperative. The failure to implement PQC allows the accumulation of a "privacy debt" that will eventually bankrupt the concept of private life for an entire generation. By analyzing the intersection of HNDL and state responsibility, this study aims to define the contours of a new "right to cryptographic integrity" as a subset of the right to privacy.

Methodology

This research utilizes a qualitative doctrinal legal analysis to assess the scope of state due diligence obligations in the face of quantum threats. The primary legal framework is drawn from the jurisprudence of the European Court of Human Rights (ECtHR) and the UN Human Rights Committee regarding the positive obligations of states to protect privacy. The study synthesizes these legal standards with the "Schmitt Analysis" of cyber operations to determine if the retroactive nature of HNDL alters the assessment of "invasiveness" and "severity" required to trigger state responsibility (Payne, 2016).

To ground the legal analysis in technical reality, the study conducts a review of recent literature on PQC standardization and the timeline for quantum readiness. This includes analyzing reports on the NIST PQC process and the challenges of implementing "crypto-agility" in legacy systems (Jena, 2025). The technical review serves to establish the "foreseeability" of the harm, which is a prerequisite for establishing a failure of due diligence under international law (Ollino, 2016). If the quantum threat is scientifically consensus-based and the solution (PQC) is available, the failure to act becomes a legal choice rather than a technological inevitability.

The methodology also incorporates a comparative analysis of data protection regimes, specifically contrasting the European approach (GDPR) with the US sectoral approach. This comparison highlights the "transatlantic divide" in privacy expectations and how it influences the regulation of cross-border data flows in the quantum era (Cohen et al., 2016). The study examines whether the "adequacy" decisions for data transfer frameworks could be invalidated by the HNDL threat, as the receiving jurisdiction may not provide protection against future quantum decryption.

Furthermore, the research draws on the "rational choice theory" of compliance to explain state behavior. States may be reluctant to mandate PQC because they themselves benefit from the HNDL strategy for intelligence purposes. This conflict of interest—between the state as a protector of privacy and the state as a collector of intelligence—complicates the enforcement of due diligence obligations (Kastelic, 2019). The methodology accounts for this political realism by focusing on the objective standards of international law rather than the subjective intent of policymakers.

The analysis is limited to verified academic sources provided in the uploaded corpus to ensure accuracy and prevent hallucination. It avoids speculative timelines for quantum supremacy, relying instead on the "risk-based" approach advocated in the literature, which treats the possibility of decryption as a sufficient trigger for preventative action (Mavroeidis et al., 2018).

Results

The analysis reveals that the HNDL threat fundamentally undermines the "confidentiality" principle of information security, which is a key component of the right to privacy. Technical literature confirms that RSA and ECC keys, which secure the vast majority of global digital traffic, are vulnerable to Shor's algorithm (Mavroeidis et al., 2018). While the exact date of "Q-Day" (when a CRQC becomes operational) is unknown, the HNDL strategy makes the threat immediate. Any data intercepted today is effectively "leased" privacy; it is private only until the lease expires upon the arrival of quantum capability (Jena, 2025).

From a legal perspective, the study finds that current interpretations of "interference" with privacy are static. Courts typically look for an active intrusion or a present disclosure of information. However, HNDL involves a passive collection phase followed by a delayed intrusion. The results suggest that the "harvesting" phase itself must be legally re-characterized as an interference with privacy, even before decryption occurs. This is because the act of harvesting removes the individual's control over the lifespan of their data's confidentiality, violating the principle of informational self-determination (Cohen et al., 2016).

The results also indicate a significant gap in the "due diligence" framework. The obligation of due diligence requires states to take "reasonable measures" to prevent harm (Ollino, 2016). Currently, most states rely on classical encryption standards which are known to be obsolete against future threats. The study finds that the continued endorsement of these standards by national regulators may constitute a failure to take "reasonable measures." The emerging consensus on PQC standards provides a benchmark for what is "reasonable," rendering the continued use of legacy encryption legally indefensible (Erol, 2025).

Furthermore, the analysis highlights the "attribution" challenge in HNDL scenarios. Unlike a kinetic attack or a ransomware event, an HNDL operation is silent. Attributing the harvesting of data to a specific state actor is notoriously difficult due to the anonymity of the internet (Chen et al., 2025). This attributional void makes it difficult for individuals to seek redress or for states to

invoke countermeasures. The result is a legal impunity gap where the violation of privacy occurs without a clear perpetrator to hold accountable.

The study also finds that the "crypto-agility" of critical infrastructure is dangerously low. Many systems are "hard-coded" with classical encryption, making the transition to PQC slow and costly (Jena, 2025). This technical rigidity translates into a human rights vulnerability. If a state cannot update its cryptographic standards quickly, it effectively condemns its citizens' data to future exposure. The results suggest that legal mandates for "secure-by-design" products must be updated to include "quantum-safe-by-design" requirements.

Finally, the results point to the interconnectedness of privacy and other rights. The compromise of privacy via HNDL can lead to violations of the freedom of expression (chilling effect), freedom of assembly, and non-discrimination. The "harvesting" of data creates a surveillance potential that can be weaponized for political repression, making the transition to PQC a matter of preserving democratic functionality (Kastelic, 2019).

Discussion

The "privacy time-bomb" created by HNDL necessitates a shift from a reactive to a proactive legal posture. The traditional "notification of breach" model, central to laws like the GDPR, is inadequate for HNDL. Notifying a user that their encrypted data was stolen is meaningless if the user cannot retroactively re-encrypt it. Once the data is harvested, the privacy violation is a deterministic event awaiting a technological trigger. Therefore, the focus of the law must shift from "remedy after breach" to "prevention of harvesting" through the mandate of quantum-resistant encryption.

The concept of "due diligence" offers the most robust framework for this shift. As established in the *Corfu Channel* case and elaborated in cyber law scholarship, states have a duty not to allow their infrastructure to be used for acts contrary to the rights of others (Kastelic, 2019). This implies a duty to "harden" the infrastructure against known threats. The "Crypto-Agility Mandate" proposed in technical circles—requiring organizations to maintain an

inventory of cryptographic assets and the ability to update them—should be codified as a component of the state's due diligence obligation (Jena, 2025).

This "positive obligation" extends to the regulation of the private sector. Since the vast majority of personal data is held by private companies, the state must enforce PQC standards on these entities. A failure to regulate the private sector's cryptographic transition effectively outsources the protection of human rights to market forces, which often prioritize cost over long-term security (Zafar, 2025). The state cannot absolve itself of responsibility by claiming the private sector owns the infrastructure; the state owns the obligation to protect the right.

The discussion also raises the issue of "data sovereignty." If a state's citizens' data is harvested by a foreign power, it represents a loss of sovereign control over that data. This links the right to privacy with national security. The protection of privacy thus becomes a matter of "digital sovereignty," justifying strong regulatory intervention in the market for encryption technologies (Journal of Business, IT, and Social Science, 2017).

However, the transition to PQC is not without legal risks. The implementation of new, complex algorithms could introduce new vulnerabilities or implementation errors (Jang-Jaccard, 2025). The state must balance the risk of HNDL against the risk of destabilizing current systems. This requires a nuanced "risk management" approach to due diligence, rather than a blunt mandate. Yet, the "existential" nature of the quantum threat to privacy suggests that the bias should be towards rapid adoption of PQC (Erol, 2025).

The "transatlantic divide" on privacy may widen in the quantum era. The EU, with its strong fundamental rights focus, may move faster to mandate PQC to protect "informational self-determination." The US, with its focus on "reasonable expectation," may lag if courts rule that users assumed the risk of future decryption (Cohen et al., 2016). This divergence could fragment the global digital economy, as data flows from the EU to the US could be blocked if the US is deemed "quantum-unsafe."

Ultimately, the HNDL threat exposes the fragility of digital rights. Rights that depend on code are only as strong as the code itself. As the code becomes

obsolete, so too does the effective enjoyment of the right. The role of the law is to ensure that the code evolves to maintain the right. This requires a "legal agility" that matches the "crypto-agility" of the technology sector.

Conclusion

The "Harvest Now, Decrypt Later" strategy represents a fundamental challenge to the right to privacy, transforming the theoretical possibility of future decryption into a present-day violation of human rights. The current international legal framework, while possessing the necessary principles in the form of "due diligence" and "positive obligations," has failed to operationalize them in the context of the quantum threat. The result is a regulatory complacency that allows the systematic accumulation of global private data by adversarial actors.

To avert a catastrophic collapse of privacy in the post-quantum era, states must recognize a positive obligation to mandate "quantum readiness." This involves legally enforcing the adoption of Post-Quantum Cryptography in critical infrastructure and personal data systems. The "Crypto-Agility Mandate" is not just a technical specification; it is a legal requirement derived from the duty to protect the integrity of private life.

The transition to PQC is the only viable remedy for the HNDL threat. Legal remedies such as lawsuits or sanctions are ineffective against a threat that operates retroactively and anonymously. The only protection is prevention. By establishing a robust standard of due diligence that includes quantum safety, the international community can ensure that the right to privacy survives the quantum leap. The time to act is not when the quantum computers arrive, but now, while the encryption still holds.

REFERENCES

Chen, H., Coco, A., Rotondo, A., & Ying, Y. (2025). *The Attribution of Cyber Operations to States in International Law*. Geneva Centre for Security Policy (GCSP).

Cohen, J. E., de Witte, B., & Purnhagen, K. (2016). Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. *International Journal of Constitutional Law*, 14(1), 220–229.

Erol, V. (2025). The Strategic Imperative of Quantum Readiness: A Comprehensive Review of Post-Quantum Cryptography. *Preprints.org*.

Jang-Jaccard, J. (2025). Practical Challenges in Executing Shor's Algorithm on Existing Quantum Platforms. *arXiv*.

Jena, J. (2025). The Quantum Security Deadline: Building Crypto-Agility Against 'Harvest Now, Decrypt Later' Threats. *European Journal of Computer Science and Information Technology*, 13(52), 35-52.

Journal of Business, IT, and Social Science. (2017). Cybersecurity and International Law: Defining State Responsibility for Cross-Border Cyberattacks. *Journal of Business, IT, and Social Science*.

Kastelic, A. (2019). *Inducing compliance with international law in cyberspace – State responsibility, countermeasures and the obligations of due diligence*. White Rose eTheses Online.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal on Advanced Science, Engineering and Information Technology*, 8(3), 991-998.

Ollino, A. (2016). *Due Diligence Under International Law: Reappraising its Scope, Functions and Limits* (Doctoral dissertation). Università degli Studi di Milano-Bicocca.

Payne, T. (2016). Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. *Lewis & Clark Law Review*, 20(2), 683-715.

Zafar, A. (2025). Quantum Computing in Finance: Regulatory Readiness, Legal Gaps, and the Future of Secure Tech Innovation. *European Journal of Risk Regulation*, 1–20.