



TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

The Dark Side of Encryption: When Privacy Protects Crime

An in-depth exploration of the fact that the very technology that helps in protecting our information can also be used to protect criminal activity in the digital era.

By **Zahida Ashraf** | Published: July, 2026

✉ ashrafzahida20@gmail.com | Position: Information Technology Student

Introduction

Encryption is frequently heralded as the foundation of contemporary digital security - securing banking transactions, personal messages, and more. However, behind its safeguarding cover is a looming menace: the same technology that maintains privacy could also allow crime to thrive in the shadows.

In Pakistan where digital uptake is fast gaining momentum, the friction between privacy and security is now becoming more apparent -and more pressing.

"The stronger our privacy tools become, the harder it is to see who might be hiding behind them."

Technology Overview

In its simplest form, encryption converts data that can be read into coded information, which can only be read by authorized personnel. Other technologies such as end-to-end encryption (E2EE) require that not even service providers can access user messages.

The emergence of digital banking, freelance websites, and e-commerce in Pakistan has led to the growth of dependency on encryption. On one hand, this enhances cybersecurity, but on the other, it introduces blind spots to regulators and law enforcement agencies that do not have the tools or legal frameworks to access encrypted data, when need be.

Key Findings & Impact

Current world wide cybersecurity news indicates that more than 70 percent of web traffic has become encrypted, which has greatly curtailed the traditional methods of surveillance. On the one hand, this improves privacy of users but, on the other hand, makes it harder to detect and prevent cybercrime.

In Pakistan, the effect is two-fold:

1. Negative: There is a growing use of encrypted communication platforms in fraud and abuse and fraud as well as financial offenses.
2. Positive: Secure digital ecosystems promote fintech development, teleworking and cross border business.



Figure 1: Encryption strengthens digital privacy by securing data through complex codes, but the same technology

What's Next?

Encryption probably will have a fine balancing act in the future. New solutions like the concept of lawful access frameworks and AI-driven threat detection are expected to detect suspicious behaviour without fully violating the privacy of users.

In the case of Pakistan, the way to go is through the interplay of tech firms, government agencies, and cybersecurity professionals. Digital forensics renewed cyber laws, and awareness among the people will be key in manoeuvring through this complicated landscape.

About the Author

Zahida Ashraf is a technology writer and software engineer specializing in cybersecurity and new digital trends. She investigates the nature of innovation, ethics and policy in contemporary IT systems. They can be reached at ashrafzahida20@gmail.com.

Keywords: Artificial Intelligence; Cybersecurity; IoT; Software Engineering; Pakistan Tech

References

- [1] SentinelOne (2026) *Key Cybersecurity Statistics for 2026*, available at: <https://www.sentinelone.com>
- [2] Cobalt (2025) *Top Cybersecurity Statistics for 2026*, available at: <https://www.cobalt.io>