INDIA SOUTHEAST ASIA EMEA
ET CIO.com ET CIO.com India • Southeast Asia

Artificial Intelligence • 3 Min Read

AI innovation is accelerating - Can India's data protection keep pace?

Artificial intelligence offers significant benefits across various industries and governance. Organizations must prioritize data protection and infrastructure security for responsible AI deployment. India's rapid AI adoption necessitates adherence to the DPDP Act's requirements. Companies need to integrate security and compliance from the outset of AI projects. Genuine progress lies in deploying AI while protecting data and accepting accountability.

Govind Rammurthy • • ETCIO
Published On Jul 16, 2026 at 08:02 AM IST

Artificial Intelligence has rapidly evolved from an emerging technology into a fundamental driver of innovation across industries. It has accelerated drug discovery, improved diagnostic accuracy in radiology, enabled predictive analytics for disease prevention, and transformed governance efficiency. These aren't theoretical benefits; they're documented impacts affecting millions.

As AI adoption continues to accelerate, however, innovation must be matched by responsibility. Organizations deploying AI today carry obligations that extend far beyond technical capability to data protection, organizational security, and ethical deployment.

AI's healthcare impact is particularly notable. Diagnostic AI systems now match or exceed human radiologists in detecting certain cancers early. Drug discovery timelines that previously took years now compress to months. Personalized medicine becomes possible when AI analyzes individual genetic and medical histories to recommend treatments. In India, AI-powered health systems now reach rural areas where specialist doctors remain scarce, democratizing access to diagnostic intelligence.

Government applications are equally transformative. AI processes millions of documents in policy analysis, identifies fraud patterns in procurement systems, and optimizes resource allocation for public services. The Indian government's use of AI for governance, DPDP compliance, and citizen services represents legitimate progress toward more efficient administration.

Yet these same capabilities create obligations that many organizations inadequately address.

The responsibility challenge begins with data - AI systems require massive datasets to train effectively. Those datasets often contain sensitive information - medical records, personal financial data, behavioral patterns. Organizations deploying AI must ask: How is this data protected? Who has access? Can it be exfiltrated? Data loss prevention becomes critical infrastructure, not optional security.

When AI processes healthcare data, that data cannot leak through insecure APIs, unencrypted storage, or unmonitored endpoints. Organizations must implement comprehensive data protection that monitors information flow through AI pipelines, restricts unauthorized access, and audits who touches sensitive data at every stage.

Infrastructure security represents another responsibility dimension - AI systems themselves become targets. Attackers can poison training data, manipulate AI outputs, or compromise model integrity. Organizations must protect AI infrastructure with the same rigor applied to critical systems. Endpoint protection monitoring all access to AI systems, network segmentation preventing unauthorized lateral movement, and behavioral analysis detecting anomalous access patterns are no longer optional - they're fundamental to responsible AI deployment.

The India context makes this especially urgent - India is rapidly adopting AI across healthcare, finance, governance, and education. The DPDP Act requires organizations processing Indian citizens' data to implement reasonable security. When that data feeds AI systems, "reasonable security" must account for the amplified risks AI creates. A data breach affecting 1,000 people is serious. When that data trained an

AI system used to make decisions about thousands of other citizens, the blast radius expands dramatically.

The uncomfortable responsibility: Organizations must decide whether they're truly equipped to deploy AI responsibly. Building an AI system requires data scientists and ML engineers. Deploying it responsibly requires security teams, compliance specialists, and privacy advocates from the beginning - not added afterward. It requires asking difficult questions: Can we ethically collect this data? Can we protect it adequately? What happens if our model is wrong? Who bears responsibility when AI decisions cause harm?

The global technology industry has celebrated AI's capabilities while under-investing in the security and governance infrastructure supporting responsible deployment. India has an opportunity to learn from this pattern - to adopt AI's benefits while insisting from the beginning that organizations accept full responsibility for the data they process and the decisions their AI systems enable.

AI Appreciation Day should celebrate genuine progress. But the progress that matters most isn't technical sophistication. It's whether organizations deploy AI in ways that protect data, maintain transparency, and accept accountability for outcomes. That's the responsibility that separates innovation from recklessness.

The author is Govind Rammurthy, CEO and Managing Director, eScan.