ILLUSTRATION: **ZARIF FAIAZ**

Data frontiers: where does Bangladesh fit in the global privacy debate?

FROM PAGE 33

multiplied globally, with the OECD noting that some localisation is viewed as useful and uncontroversial, while other forms are seen as barriers to the digital economy. The WTO has also pointed to the continued rise in data regulation measures, including increases in data localisation, framing it as part of a broader policy shift affecting trade.

This is the global stage on which Bangladesh is writing its rules.

BANGLADESH'S NEW DATA REGIME AND THE PROMISES IT MAKES

Bangladesh's Personal Data Protection Ordinance was gazetted in November 2025, according to the Bangladesh Government Press archive, marking a formal milestone after years of debate. DataGuidance, which tracks privacy developments, described the ordinance as effective from 6 November 2025, positioning it as a nationwide framework for personal data processing.

Public-facing explanations of the new laws emphasised rights. Bangladesh Sangbad Sangstha reported that citizens would have rights including access, correction and deletion, and it also highlighted a right to restrict automated decisions made using personal data. Prothom Alo reported that a national data management authority would be established under the National Data Governance Ordinance to formulate data policies, ensure compliance and resolve complaints, while also guaranteeing security across national databases and software systems.

The Daily Star, in its early coverage of the ordinances, highlighted the idea that people are owners of their data, while the state and companies act as custodians or processors. In principle, that is a significant shift in framing. Ownership language, even if contested by lawyers in other jurisdictions, signals that the individual is not meant to be treated as a passive resource.

Yet the practical impact of any privacy law depends not on slogans but on details: who the regulator answers to, how exemptions are written, whether cross-border rules are workable, and what enforcement looks like when powerful actors breach the rules.

Those questions quickly became central to the Bangladeshi debate.

IMAGE: **LIANHAO QU/ UNSPLASH**

CONTROL, CONSULTATION, AND THE FEAR OF EXECUTIVE OVERREACH

From the start, civil society groups and some legal analysts warned that Bangladesh's new framework risked being too concentrated in executive hands. Transparency International Bangladesh criticised what it described as a hasty approval process without expert consultation and questioned whether the proposed authority would be independent and aligned with global practices. The Daily Star reported similar concerns, including criticism that key international data protection principles were missing or weak, and that the structure could create a crippled regime if not amended.

> Bangladesh can become a credible, rights-based player in the global data economy, or it can drift into a model where "protection" is promised but "control" becomes the lived experience.

A further worry has been the scope of government direction. Prothom Alo reported expert concerns about provisions that would allow the government to issue directives to the authority on grounds such as sovereignty, security and public order, and to issue orders related to data storage or transfer in urgent cases, which critics argued could grant unchecked power without judicial oversight. Article 19 has repeatedly argued Bangladesh should adopt a data protection regime grounded in international human rights law, warning against structural weaknesses that could enable surveillance rather than protection.

These arguments do not occur in a vacuum. Bangladesh's recent history of digital regulation has been shaped by controversy around laws used to police speech and online activity. Reuters reported in 2023 that Bangladesh would tone down parts of the Digital Security Act after long-standing criticism that it was draconian and could curb dissent. Separately, debate around cybersecurity law has continued, with proposals to recognise internet access as a civic right receiving attention in regional coverage.

Privacy law, in other words, is being built in a context where trust must be earned, and where people have reasons to scrutinise any broad state discretion.

DATA LOCALISATION AND THE ECONOMICS OF BEING PLUGGED INTO THE WORLD

The most explosive technical issue in Bangladesh's privacy debate has been data localisation. For governments, localisation can seem like a straightforward response to sovereignty concerns. Keeping data in-country can make it easier to enforce local laws, compel access, and build domestic data centres. It can also be sold politically as a way of preventing foreign surveillance.

For businesses, especially those using global cloud infrastructure, strict localisation can be expensive and destabilising. It can force companies to rebuild systems, complicate cybersecurity strategies, and create fragmentation where data that needs to move across borders for fraud detection, customer support or resilience is boxed in by law.

That tension appears to be driving rapid adjustment in Dhaka. In early January 2026, The Daily Star reported that the government removed broad localisation requirements for technology companies and scrapped jail terms for violations by tech firms, including global platforms, through amendments approved by the advisory council. Other reporting suggested localisation would apply more narrowly, such as to critical information infrastructure, rather than to all categories of data by default.

The speed of this shift matters. It suggests the government is attempting to reconcile two goals at once: signalling sovereignty and citizen protection, while avoiding rules that could scare off investment or break the architecture that modern services rely on.

Globally, that balancing act has become the norm. The EU promotes strict rights protections while still permitting cross-border transfers through adequacy decisions and legal mechanisms. The United States has focused on enabling data flows for commerce while negotiating safeguards in specific contexts.

SEE PAGE 35