LAW OPINION

New data laws in Bangladesh: A CRITIQUE

SAJID HOSSAIN

Bangladesh has entered a new phase in its digital governance story with two Ordinances, namely, The *Personal Data Protection Ordinance 2025* (PDPO) and the *National Data Management Ordinance 2025* (NDMO). Their appearance, almost devoid of public discussion, invites reflection: are we witnessing the long-delayed codification of digital rights, or the rise of a data-centric State?

Firstly, section 3 of the NDMO declares that its provisions shall take precedence over any other law, contract or instrument in matters relating to the collection, storage, processing, security and identification of persons of personal data, and the overall management and interoperability of national data. In one sweep, the NDMO asserts primacy across virtually the entire domain of data governance. Contrast this with Europe, where the *General Data Protection Regulation* (GDPR) operates under the Charter of Fundamental Rights, which enshrines respect for private life and protection of personal data as fundamental rights. The Court of Justice of the European Union (CJEU) has struck down legislation that intruded too far into those rights, notably in *Digital Rights Ireland* and *Tele2 Sverige AB*. In the European model, secondary legislation bends to rights; in ours, the NDMO begins with a supremacy clause.

Institutional design reinforces that contrast. Under section 8(2) of the NDMO, the National Data Management Authority is established as a statutory body attached to the Prime Minister's Office. Under section 23, it designs and operates the nation's data architecture, including digital interoperability systems and an identity layer linking core registers, and also enforces compliance and imposes administrative penalties under sections 42–45. Under the GDPR, by comparison, Member States must create independent supervisory authorities that act *"with complete independence"* in monitoring the law's application. In *Commission v Germany* (ECJ C-518/07) and *Commission v Hungary* (C-288/12), the CJEU held that such authorities must act with complete independence from any external influence, including direct or indirect influence of the State. Bangladesh's new Authority, however, sits within the executive branch. It is simultaneously an architect, operator and enforcer, effectively acting as the referee and a player at once.

Perhaps the most ambitious feature lies in the identity layer mandated by section 23 of the NDMO and its Schedule. This unified system is designed to connect a citizen's National ID, passport, tax identification number and other key registers. The intended benefits are administrative efficiency and easier access to public services. Yet technical unification also brings constitutional risk. When every register speaks to every other, the State gains the capacity to reconstruct a person's entire life-trajectory – where one lives, travels, works, banks and interacts online.

Under GDPR Articles 5 and 25, personal data must be collected for specific, explicit and legitimate purposes and be limited to what is necessary. By contrast, the Ordinances contain no explicit, general-purpose duties of purpose-limitation and data-minimisation binding on State processing. What promises frictionless governance could, without constraint, evolve into frictionless surveillance.

Then there is also the question of how these far-reaching measures arrived. Both Ordinances were promulgated under Article 93(1) of the Constitution, authorising the President to issue ordinances when *"circumstances exist which render immediate action necessary"*. Parliament stands dissolved; yet through this route, Bangladesh has now enacted the most comprehensive data-governance regime in its history. A potent query thereby arises: was there truly an extraordinary necessity justifying the use of that power for something this foundational?

A framework that will shape the country's digital constitution deserves the full sunlight of parliamentary debate. The GDPR took years of public consultation and legislative negotiation before it was argued into existence through committees, parliaments and courts – proposed in 2012, adopted in 2016, effective in 2018. Our twin Ordinances arrived in one November gazette by executive fiat. While Ordinances are constitutionally valid, they are simply not constitutionally deliberative. The difference matters when the legislation in question defines the relationship between citizen and State in the digital era.

Furthermore, the Authority's remit effectively makes the Bangladeshi State the most consequential data controller in practice. Under the NDMO, it manages citizen-data life cycles, coordinates integration across ministries and enforces compliance. Section 24(1) of the PDPO creates consent exemptions covering, *inter alia*, national security, crime control, taxation, public interest, and public-health emergencies. Though sections 24(2) and (4)– (6) limit pure blanket use, their sheer scope risks leaving much state data-processing subject to internal rather than independent oversight.

Hence, for instance, when a private bank mishandles data, the Authority may sanction it. But when a ministry misuses citizen data, will an Authority seated in the Prime Minister's Office do the same? The combination of broad statutory exemptions and executive-controlled enforcement produces a paradox: Big Tech may now face tighter rules, but Big State remains largely self-regulated. This is not to deny the potential gains of improved service delivery and data localisation. But these are infrastructural advantages, not rights guarantees. The Ordinances give citizens the right to access their data, but not always the right to refuse its use.

However, several correctives are still possible. The Authority's independence should be entrenched in statute, modelled on GDPR-style safeguards. Purpose-limitation and data-minimisation rules should bind state agencies as firmly as they bind private controllers, and the Ordinances should advance to Parliament as full Acts preceded by consultation with technologists, civil society and the legal community. A modern data-protection framework should operationalise privacy as a core civil right, not subordinate it to infrastructural convenience.

Bangladesh now stands at a crossroads. We can treat these Ordinances as the culmination of our digital-governance journey, or as its beginning – a chance to craft, through public debate, a data regime that protects citizens not only from corporations but from the overreach of the State itself. The difference between a *GDPR moment* and a *data-state moment* lies not in the technology we adopt, but in the constitutional temperament with which we wield it.

Bangladesh now stands at a crossroads. We can treat these Ordinances as the culmination of our digital-governance journey, or as its beginning – a chance to craft, through public debate, a data regime that protects citizens not only from corporations but from the overreach of the State itself.

The writer is an Advocate specialising in corporate, commercial and technology law.

BRIEF LAW REVIEW

The draft Telecommunication Ordinance 2025

ABRAR BIN SHOUKAT ALVI

For decades, Bangladesh's digital network has operated under the constant threat of arbitrary executive interferences. Access to the internet could be severed without notice or remedy whenever there emerged any political tension within the country.

Importantly, Bangladesh lacked any explicit statutory basis for such interferences. Orders were conveyed orally or through encrypted messages from the National Telecommunication Monitoring Centre (NTMC) to operators, with no publication or review. The result was a legal vacuum, where fundamental rights under the Constitution, of being treated only in accordance with law and the right to free speech, expression could be suspended by administrative discretion alone.

Against that backdrop, the draft Bangladesh Telecommunication (Amendment) Ordinance 2025 presents quite a transformative development. It says that "no telecommunication connection, service or internet access shall be shut down, disrupted or restricted under any circumstances". This mandate, if materialised, will be in line with global jurisprudence on freedom of expression and information protected by Article 19 of the International Covenant on Civil and Political Rights (ICCPR). It will also stand in alignment with Bangladesh with the position of the UN Human Rights Council, which in 2022 reaffirmed that blanket internet shutdowns can never be justified.

However, a single prohibitory clause does

not take us far. From a governance perspective, the new ordinance should also introduce institutional safeguards to ensure that the promise of non-interference survives changes in political will. While the draft law has provisions for parliamentary and judicial oversight, there is still room for improvement. First, in line with the EU Digital Services Act 2022, the operators, independent of government regulators, should be made obligated to publish reports detailing any governmental request affecting network operators. This will potentially ensure transparency and accountability in governance and ensure their conformity with the right to information.

Furthermore, an independent digital rights commission to investigate violations, audit state use of digital powers, and provide remedies could also be established. Similar commissions exist under the African Union Model Law on Access to Information (2013). A digital compensation fund should also be formed to provide redress when governmental action or inaction causes any quantifiable loss to businesses. Finally, the draft Ordinance should be harmonised with the data protection laws in order to ensure that the right to connectivity complements the right to privacy under Article 43 of the Constitution.

Internationally, Bangladesh has often been cited by Access Now and Article 19 for its opaque handling of digital governance. With the new ordinance being passed and implemented, the country could potentially transform from a case study in digital authoritarianism into a regional model of digital democracy.

The writer is student of law at Bangladesh University of Professionals.

JUDGMENT REVIEW

Consultation with the Chief Justice in appointing SC judges

ABUZAR GIFARI

Article 95(1) of the Constitution of Bangladesh mandated the President to consult the Chief Justice (CJ) when appointing Supreme Court (SC) judges. This requirement was removed by the 4th Amendment in 1975 but reinstated by the 15th Amendment in 2011. This issue was first examined in *Bangladesh* v *Idrisur Rahman*, reported in 29 BLD (AD) 79, also known as the *Ten Judges' case*. The Appellate Division (AD) ruled that consulting the CJ was a necessary "constitutional imperative or convention" for appointing SC judges, even when this requirement was omitted by the 4th Amendment. Evidence shows that all SC judges were appointed after consulting the CJ, except once in 1994, confirming that such consultation has crystallised into a customary practice. The Court also held that considering CJ's opinion with primacy is crucial for judicial independence, a principle enshrined in the rule of law.

As the 8th Amendment case held the rule of law as a basic structure of the constitution, the Prime Minister or President cannot violate it. Under Article 48(3), the President must act on the Prime Minister's advice when appointing SC judges. Then, what would happen when the opinion of the CJ and PM comes into conflict? In this regard, the Court established a bifurcated consultation process: first, the CJ's opinion would have primacy for evaluating legal acumen and suitability of the judges concerned, and, secondly, the Prime Minister's opinion would have primacy for assessing antecedents. However, this process left ambiguity regarding situations where the CJ's recommendation was not accepted by the executive.

Recently, this finding was modified in *ABM Altaf Hossain and others* v *Bangladesh* (2023). The Appellate Division ruled that in case of conflict between the CJ's and the executive's opinions, neither would have primacy, and the appointment would not proceed. This departure from long-standing judicial convention relied on the Indian *SP Gupta Case* (1982), where the Indian Supreme Court held

that in case of conflict, neither opinion had primacy. However, this rule was later overruled in India by the *Advocates-on-Record Case* (1993), where the CJ's opinion was given primacy. Although the latter case was also referred to in the *ABM Altaf Hossain* case, reliance was primarily put on the *SP Gupta* case. In my opinion, this can be seen as abusive selective borrowing of a constitutional idea, not justified by contemporary comparative constitutional law theories.

The Court criticised the Ten Judges' case for rendering primacy to the executive through the bifurcated consultation process and aimed to uphold judicial independence. However, in doing so, the Court rather inadvertently strengthened the executive's power over the judiciary. For instance, if the CJ recommends a candidate and the Prime Minister rejects it, the candidate would not be appointed, effectively giving the Prime Minister dominant authority in judicial appointments.

Indeed, the Court did not provide strong legal reasoning for deviating from its precedent. It only cited the absence of "political motivation" in the present case and contrasted it with the *Ten Judges'* case. A well-substantiated justification was required for effecting such significant change in the constitutional jurisprudence.

The writer is Lecturer in the Department of Law and Land Administration, University of Rajshahi.