The Daily Star
FOUNDER EDITOR: **LATE S. M. ALI**

# Army cooperation with ICT trials vital

## Meaningful reform of security agencies can prevent reversion to old practices

We welcome the Bangladesh Army's decision to act on the warrants issued by the International Crimes Tribunal (ICT) against 16 in-service ranking officers recently indicted for crimes against humanity, including enforced disappearance and torture in custody. Its announcement in this regard—that all but one of those accused officials have been placed under custody—has reassured observers and the public, dispelling social media rumours meant to create sensation and stir unwarranted political tension. These trials are vital to ensuring justice for the many victims of cruel and inhumane suffering.

It was also reassuring to hear Adjutant General Md Hakimuzzaman affirm, at a press briefing held at the Army Headquarters on Saturday, that "Bangladesh Army respects all laws recognised by the Constitution." We hope that this spirit will be carried through in all its future actions. The nation and the international community will be watching closely to ensure that the army's public pledge to cooperate with the ICT's judicial process is followed through. We can recall that the United Nations fact-finding mission's report on the July uprising atrocities also called for ensuring accountability of members of security agencies. Any issue with technical clarity in the ICT Act, hopefully, will not affect the administration of justice.

We also note the adjutant general's assertion that those named by the ICT for alleged crimes were charged for their actions while working at the Directorate General of Forces Intelligence (DGFI) and the Rapid Action Battalion (Rab), and that these agencies at that time were not under the Army HQ. Distancing the accused from the army as an institution certainly deserves due consideration, as the DGFI functions under the Prime Minister's Office—currently under the Chief Adviser's Office—and Rab is an arm of the police.

Here comes the question of how the army as an institution can protect its sanctity and integrity from those who may tarnish it by committing criminal acts during their secondment to other agencies. An institutional mechanism of rigorous screening before their reinstatement must be developed. The question of differentiating between the army and its officers serving in various security agencies outside the force also reminds us of the need to reform these agencies.

There must be effective legal deterrents to prevent politicians from misusing security agencies—particularly the DGFI—for partisan purposes. Equally important is ending the abuse of power and impunity these agencies have long enjoyed on flimsy security grounds. Besides political workers, student activists, rights defenders, and academics, we in the media have also experienced DGFI's overreach. It intimidated newsrooms so often that a climate of fear persisted for quite a long time, affecting press freedom.

We echo the calls made by some civil society organisations such as the Transparency International Bangladesh and the Human Rights Forum Bangladesh that the interim government must initiate meaningful reform of these security agencies, so that the incoming political government post-elections can carry the process forward. We need reforms that can prevent a reversion to the old practices of power abuse and the weaponisation of these agencies by political masters.

# Leave no room for misuse

## New data protection and governance ordinances need consultations

The Advisory Council's approval of the Personal Data Protection Ordinance, 2025 and the National Data Governance Ordinance, 2025 is a significant development in Bangladesh's digital governance. While there is an undeniable need for a comprehensive legal framework to protect personal data, there are concerns, as voiced by the likes of Transparency International Bangladesh (TIB), about the possibility of the laws being misused.

According to TIB, the two ordinances with some questionable provisions were approved hurriedly, without adequate expert consultations or stakeholder engagement, which is concerning. During the last regime, stakeholders and experts had criticised the draft data protection law, particularly for the way it enabled surveillance. This time, an inclusive and extensive dialogue was expected, especially given its implications for privacy, civil liberties, and state accountability. While that expectation was not met, the dilution of internationally accepted data protection principles—such as lawfulness, transparency, and confidentiality—raises serious concern.

Especially alarming is the draft's subsection 15(4), which allows exemptions for data controllers, as well as Section 24, which gives access to personal data for "crime prevention" without judicial oversight. These provisions have the potential to become tools for surveillance and control, leading to violations of constitutional privacy rights. Extensive powers have been granted to the proposed National Data Management Authority, which will operate under the office of the prime minister or chief adviser. Furthermore, Section 23 mandates all "significant data controllers" to appoint a Chief Data Officer (CDO) but fails to specify whether these officers will be accountable to any government authority. Section 24 allows the government to access personal data without consent for reasons such as national security, defence, public order, or crime prevention and investigation—without clearly defining these terms, thereby heightening the risk of misuse. Section 50 empowers the government to issue directives to the authority on matters concerning sovereignty, security, public order, or foreign relations, while Section 55 authorises it to issue any order regarding data storage or transfer in cases deemed urgently necessary.

Undoubtedly, some provisions of the ordinances—mandating informed consent, securing sensitive data, empowering citizens with rights over their data, and introducing penalties for breaches—are crucial for safeguarding user privacy. But the lack of transparency in their drafting and the risk of increased state surveillance are issues that must be addressed. The government should pay heed to TIB's call not to enforce the ordinances now without meaningful consultations with experts and stakeholders.

# We need a data privacy law that serves the people, not power

**Barrister Khan Khalid Adnan**
*is advocate at the Supreme Court of Bangladesh, fellow at the Chartered Institute of Arbitrators, and head of the chamber at Khan Saifur Rahman and Associates in Dhaka.*

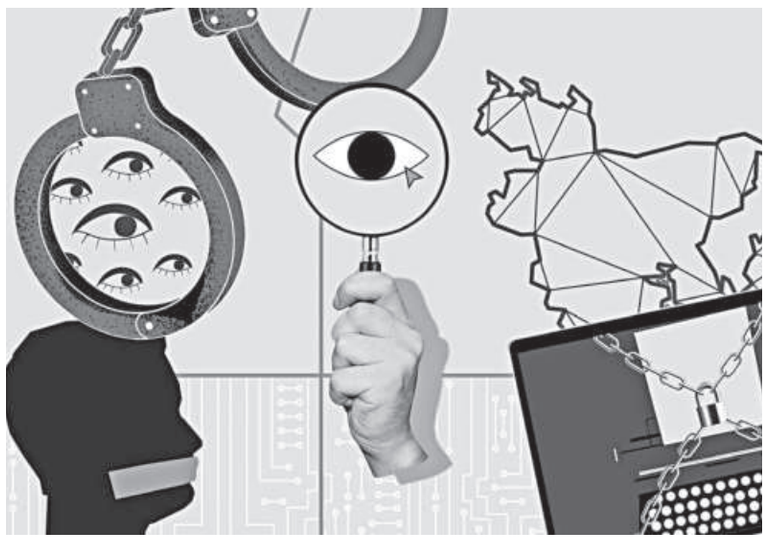
**Azfar Adib**
*is senior member at the Institute of Electrical and Electronics Engineers (IEEE) and PhD candidate at Concordia University, Canada.*

**KHAN KHALID ADNAN** *and* **AZFAR ADIB**

Bangladesh stands on the cusp of a defining choice for its digital future. On October 9, the interim government approved the long-anticipated Personal Data Protection Ordinance 2025, aimed at protecting citizens' data privacy and creating a comprehensive legal framework to regulate the collection, storage, processing, and sharing of personal information in the digital sphere. The ordinance promises consent, transparency, and accountability, gesturing towards the gold standard set by the EU's General Data Protection Regulation (GDPR). However, a proposed draft circulating online shows that the ordinance has deviated at least in certain respects. The draft sketches a regulator, data breach duties, and individual rights. Yet beneath the headline goals lie structural flaws that highlight the need for further checking control reflexes and turning policy slogans into enforceable guarantees.

Let's begin with exemptions. Section 28 of the draft creates a wide escape hatch for crime-fighting, investigations, regulatory work, statistics, and even open-ended categories that regulators can later expand. Interestingly, the proposed version did not include the terms "national security" or "public order" under the exemption category, but these have been included into the approved ordinance. Given the country's history of legal abuse, such exemptions risk legitimising arbitrary surveillance, discriminatory profiling, and control over information, particularly in situations involving political dissent or journalistic work. Without clear safeguards and effective independent oversight, activists, journalists, and minority communities may remain exposed to abuse and retaliation. The solution is straightforward: every exemption must comply with the principles of legality, necessity, and proportionality—supported by judicial approval, clearly defined purposes, independent audit mechanisms, and regular public transparency reports.

Regulatory independence is the second fault line. The draft grants the National Data Governance and Interoperability Authority broad powers, yet tethers its major actions to prior government approval, including for standard operating procedures and core classifications. The remedy for this is both boring and vital: appointment by parliament with cross-party consent, fixed terms, protected budgets, and transparent rule-making that cannot be vetoed by the Cabinet Division. Such administrative hygiene is also enshrined in Article 52 of the GDPR, which hardwires independence into the supervisory model.



VISUAL: **ANWAR SOHEL**

Cross-border data transfers are the third trouble spot. Section 34 ties data flows to a new state-run taxonomy and hints at fees on data generated in Bangladesh, while Section 35 enables transfers for trade and reciprocity without a clear risk assessment framework. That is an invitation to rent-seeking, forum shopping, and regulatory arbitrage. A credible system needs a simple ladder—adequacy decisions for trusted destinations, standard contractual clauses for everyone else, binding corporate rules for global groups, and explicit risk assessments for high-impact processing. The policy shelf already has these tools. They are tested, interoperable, and predictable. Use them.

Localisation deserves a reality check. Data residency can be legitimate for certain categories such as defence or critical registries. Mandating wholesale localisation through broad classifications is not a good strategy. Bangladesh should localise where risk demands it, and otherwise optimise for secure, lawful, and fast transnational data flows. If the government still wants an industrial policy dividend, tie any localisation to clear technical benchmarks and measurable service gains rather than symbolic flags on servers.

Proper infrastructure matters. The country already runs a tier-4 National Data Centre at Bangabandhu Hi-Tech City (which has been renamed after the 2024 uprising) and has a sovereign government cloud. Private-sector builds are coming online. These are serious assets that can anchor a privacy-first economy if they meet global standards and deliver reliable uptime at competitive price points. That means formal certification, independent audits, smart peering, and energy-efficient operations. It also means aligning operator practices with international reliability norms.

Connectivity is a multiplier. The new SEA-ME-WE 6 cable will expand capacity and improve path diversity, reducing the fragility we saw when previous systems went dark and traffic had to limp through terrestrial routes. The policy task is to accelerate landing timetables, streamline repairs, and guard against single-vendor choke points. Meanwhile, caches and content delivery networks should be encouraged, not disrupted by ad hoc directives. Local edge keeps costs down and speeds up the internet for everyone. So, publish a cache policy, make it stable, and get out of the way.

Satellite communication is no longer a side quest. With Starlink now in the market, the government can require open peering and transparent quality metrics while removing regulatory frictions that block enterprise and rural adoption. A satellite backbone that rides above terrestrial politics raises the cost of network shutdowns and creates redundancy during disasters. Write those expectations into licensing and procurement so that resilience becomes a deliverable.

Rights without remedies are just vibes. The final law should give citizens fast redress. That includes a clear path to complain, statutory deadlines for decisions, meaningful compensation, and collective actions for systemic abuse. Timely breach notification is part of that social contract. Seventy-two hours to the regulator is a sensible default already supported by global practice. Pair it with a duty to notify affected users when the risk is real.

The government has already drawn criticism for the hurried approval of the ordinance. What it should do is put the text through a real public feedback mechanism, publish a dispositions memo showing what has changed and why, and invite external security testing of the regulatory machinery before it goes live. What should an ideal situation look like? A regulator that can say no to executive overreach. Exemptions that are narrow, time-bound, and court-supervised. Cross-border rules that companies can implement without guesswork. Local infrastructure that competes on reliability and price, not proximity to a ministry. Connectivity that is diverse by design. Breach duties that actually inform people. A playbook that treats citizens as rights holders, not data sources for administrative convenience.

Bangladesh can still choose that path. Build a regulator that can stand up to politics. Replace vague exceptions with hard tests and hard logs. Swap fuzzy localisation for practical safeguards that travel across borders. Double down on world-class infrastructure and stable connectivity policy. We must remember that a privacy theatre will not age well; a proper rights law will.

# *The politics of peace, sponsored by the powerful*

MIND THE GAP

**Barrister Noshin Nawal**
*is a columnist for The Daily Star. She can be reached at nawalnoshin1@gmail.com.*

**NOSHIN NAWAL**

Once upon a time, peace used to be noisy. It marched through the streets, shouted through megaphones, and dared to disturb those who mistook silence for stability. Gandhi did not fast for brand partnerships. Martin Luther King Jr did not ask his oppressors to like and subscribe. But in 2025, peace has found a new aesthetic: carefully worded, media-trained, and proudly retweeted by the very people it is supposed to hold accountable.

This year, the Nobel Peace Prize went to Venezuelan opposition leader María Corina Machado for her "tireless work promoting democratic rights." It sounds noble enough—until she thanked US President Donald Trump for his "decisive support." The same Trump who once tried to deploy the National Guard against his own citizens and dismantled USAID under the spiritual guidance of Elon Musk. Apparently, world peace is now part of his portfolio, somewhere between space tourism and meme posting.

The irony here is not subtle. In the same breath that the White House accused the Nobel Committee of "placing politics over peace," Machado graciously dedicated her prize to a man whose presidency was practically a four-year war on empathy. One could almost hear Alfred Nobel rolling in his grave, whispering, "This isn't quite what I meant by peace."

Trump, of course, responded with the self-restraint of a toddler denied dessert. He congratulated Machado, reposted her praise, and then declared that the Nobel Prize had "lost credibility." Which, to be fair, might be the first time Trump has ever been right by accident. Because if peace prizes are now handed out like influencer collaborations—complete with cross-platform gratitude and mutual back-patting—then credibility is not the only thing that has been lost.

Let's pause to admire the absurdity. Russia's Vladimir Putin, not usually known for his love of peaceful resolutions, praised Trump for "doing a lot to resolve complex crises." Israel's Benjamin Netanyahu chimed in too, hailing Trump as a global peacemaker. When the planet's most conflict-committed leaders start agreeing on who deserves a peace prize, one begins to wonder whether "peace" has been redefined to mean "PR coordination between autocrats."

This is not the first time the Nobel Committee has found itself tangled in contradictions. Obama's 2009 win for "promoting dialogue" came just months before he authorised drone strikes that did quite the opposite. But at least Obama did not dedicate his award to George W Bush. Machado's decision to thank Trump feels like the diplomatic equivalent of applauding your arsonist for keeping the fire warm.

It's not that she is undeserving of recognition; Venezuela's struggle for democracy is real, brutal, and courageous. But the optics of praising a man cheered on by Netanyahu and Putin make the whole ceremony feel less like a celebration of courage and more like a LinkedIn endorsement exchange.

Even the Nobel Committee's citation sounded as if it had been drafted by ChatGPT on polite mode: "For tireless work promoting democratic rights." You could slap that line on half the world's think tanks and three-quarters of its hypocrites. It is the kind of praise that means everything and nothing, the award equivalent of a participation trophy at the apocalypse.

Meanwhile, Trump continues his second term, still auditioning for "Most Improved Peacemaker." His administration, armed with slogans and surrounded by billionaire-turned-advisers, has reshaped global diplomacy into a corporate strategy deck. Peace, to him, is no longer a value but a deliverable, preferably one announced two days before Nobel nominations close.

And the Nobel Committee? It seems caught between nostalgia and naivety. It wants relevance in a world where activism has been rebranded as content creation. But in trying to stay modern, it has started mistaking visibility for virtue. It is no longer about who risked their life for peace; it is about who can fit "peace" into a trending hashtag without losing their donor base.

Perhaps the real tragedy is not that Trump did not win, or that Machado did—it is that the award itself has stopped meaning anything beyond optics. When activists must thank their benefactors, and world leaders must feign enlightenment for applause, peace becomes performance art. And the Nobel stage, once sacred, now looks suspiciously like a red carpet, complete with moral sponsorships and ideological brand deals.

There was a time when peace prizes embarrassed the powerful—when they provoked, irritated, and disrupted. Today, they flatter. They've gone from defiant to diplomatic, from firebrand to photo op. The new age of peace is not about ending wars; it is about editing them for prime time.

Maybe the Nobel Committee should be honest and update the prize categories: "Best Supporting Role in a Ceasefire." "Outstanding Achievement in Selective Outrage." "Lifetime Contribution to the Illusion of Global Stability." That way, at least the rest of us would know what we're applauding.

Because peace, the real kind, is not polite. It does not thank its sponsors. It does not survive on applause from Netanyahu or compliments from Putin. It does not dedicate its victories to men who once bragged about building walls.

The truth is simple: when peace starts needing permission from the powerful, it stops being peace. It becomes PR—a beautifully packaged illusion, complete with hashtags, handshakes, and a trophy for whoever looks best holding it.

**The Daily Star** Reg. No. DA 781 | **EDITOR & PUBLISHER: Mahfuz Anam** Printed by him on behalf of Mediaworld Ltd at Transcraft Ltd, 229, Tejgaon Industrial Area, editor@thedailystar.net | **Registered & Head Offices:** The Daily Star Centre 64-65 Kazi Nazrul Islam Avenue, Dhaka-1215 Phone: 09610222222 | **Newsroom:** Fax- 58156306 reporting@thedailystar.net | **Advertisement:** 01711623910 advertisement@thedailystar.net GPO Box: 3257 | **Subscription:** 01711623906 | thedailystar.net bangla.thedailystar.net/