

BANGLADESH BRIEFING

JUN - JUL 2026

Table of Contents

AN AMENDMENT OF BANGLADESH'S ANTI-TERRORISM ACT (ATA) OF 2009	1
<i>Timeline of the Anti-Terrorism Act, 2009 to 2026</i>	2
THE CYBER SECURITY (AMENDMENT) ACT, 2026: AN ANALYSIS	4
<i>Timeline: From the ICT Act to the 2026 Amendment</i>	5

An amendment of Bangladesh's Anti-terrorism Act (ATA) of 2009

On 8 April 2026, Home Minister Salahuddin Ahmed placed the [Anti-Terrorism \(Amendment\) Bill, 2026](#) before the Jatiya Sangsad. He described the legislation as concerning the banning of what he called a genocidal, terrorist organisation, and tied it directly to the movement led by the opposition and the National Citizen Party (NCP), which he said had produced a public consensus in favour of banning the Awami League's activities. The bill did not introduce new policy so much as ratify one already in force: it converted a May 2025 interim-government ordinance into permanent law, without changing its contents.

What appears, at first glance, to be a straightforward political win for the opposition (the criminalisation of a shared adversary) masks a far more troubling reality underneath. Beneath the surface justification of counterterrorism lies a law that hands the government sweeping, largely unchecked power over political life itself. This is not simply about banning one organisation; it is about the mechanism through which any organisation can be banned, and how far that ban is allowed to reach once it is imposed.

The operative change sits in Section 18 of the 2009 Act. Previously, Section 18(1) allowed government only to declare an entity banned or to list it in the schedule of proscribed organisations. The amendment allows the government to additionally ban all activities of any entity, not merely its formal existence. This shifts the law from proscribing an organisation's name and legal status to proscribing everything the organisation and its members might do.

Section 20 was broadened in parallel. The amended provision empowers government to ban the publishing or printing of any press statement made by or on behalf of a banned entity, and to prohibit publicity for that entity across mass media, online platforms and social media, as well as processions, rallies, gatherings, press conferences and public speeches. [Analysts have described this as, in effect, a comprehensive communication blackout](#) imposed on any organisation once it

is proscribed, extending the law well beyond banning a party's legal existence into banning its speech.

Legal commentators argue the combined effect of the two sections is [a transfer of authority from courts to the executive](#). [A single gazette notification under Section 18\(1\) can now suspend a party's activities](#), and [Section 20 extends that suspension across nearly every sphere of political life](#), without any prior judicial finding that the organisation meets a legal threshold for terrorism. Commentary in academic and legal outlets has described this as [a shift from courts interpreting the limits of political action toward the executive itself defining and enforcing those limits](#). A related concern is definitional: [terms such as membership and support are not clearly defined in the amended law](#), making it easier to stretch enforcement beyond the legislature's stated intent, particularly given that [the prohibition on publicity extends to online and social media activity without any proportionality test written into the statute](#).

Section 18(1) has already been used twice before the 2026 amendment, against opposite ends of Bangladesh's political spectrum, which is part of why critics see the mechanism itself as the problem rather than any single target. On 1 August 2024, [Sheikh Hasina's government used it to ban Jamaat-e-Islami and its student wing, Shibir, over alleged violence during the quota-reform protests](#), citing earlier war crimes verdicts against Jamaat; four days later Hasina was removed from office, and on 28 August [the interim government under Muhammad Yunus reversed the ban, citing lack of evidence](#). Less than a year later, the same mechanism was turned on the party that had first used it: on 11 May 2025 the interim government issued an ordinance revising Sections 18 and 20, and the next day [banned all activities of the Awami League and its affiliates pending International Crimes Tribunal trials](#), with officials noting the original 2009 Act had no provision for banning an entity's activities until this amendment closed that gap. Parallel changes to the Tribunal Act followed, enabling trial of the Awami League as an organisation itself, [with rights groups warning the new definition was broad enough to cover any political party, affiliated group, or individual judged to support, endorse, or facilitate a banned party's activities](#).

Timeline of the Anti-Terrorism Act, 2009 to 2026

- 2009: The Anti-Terrorism Act is enacted, giving government the power to declare an entity banned or list it in a schedule of proscribed organisations under Section 18(1).
- 1 August 2024: [The Hasina government bans Bangladesh Jamaat-e-Islami, Islami Chhatra Shibir and affiliated bodies under Section 18\(1\)](#), citing the quota-reform unrest and prior International Crimes Tribunal verdicts.
- 5 August 2024: Sheikh Hasina is removed from office following weeks of protest; an interim government led by Muhammad Yunus takes power.
- 28 August 2024: [The interim government reverses the Jamaat-e-Islami ban, citing lack of evidence](#).
- 11 May 2025: The interim government issues an ordinance amending Sections 18 and 20 of the 2009 Act, adding the power to ban an entity's activities and its publicity.

- 12 May 2025: [The Awami League and its affiliated organisations are banned under the revised law, pending International Crimes Tribunal proceedings against its leadership.](#)
- 8 April 2026: The newly elected parliament, led by Prime Minister Tarique Rahman's government, [passes the Anti-Terrorism \(Amendment\) Act, 2026](#), converting the 2025 ordinance into permanent law with a repeal-and-savings clause preserving all actions already taken under it.

Ministers framed the amendment as closing a technical gap rather than expanding state power. The bill's statement of objects and reasons argued that the original 2009 Act let government list an entity as banned through a gazette notification, but did not explicitly let it ban that entity's activities, so the amendment was needed to make the law more effective and up to date. Officials have consistently presented the broader 2025 to 2026 legal package as an accountability measure: holding Awami League figures responsible for abuses committed while in power, in response to demands from political parties and student organisations rather than as a tool of repression.

The bill's passage drew immediate procedural objections. Opposition Leader Shafiqur Rahman said members had received the comparative document, showing what had changed from the 2025 ordinance, [only three to four minutes before the vote](#), leaving no real opportunity to review sensitive legislation. [Speaker Hafiz Uddin Ahmad replied that the designated window for objections had already passed. The bill was then passed by voice vote](#), with the ordinance's substance left entirely unamended.

The amendments passed through parliament swiftly as it introduced no new substantive rules but rather ratified a fifteen month old ordinance. This allowed the government argue there was little left to debate, the comparative document notwithstanding. At the same time, the vote rode on what officials repeatedly called a public consensus against the Awami League, a framing that cast any objection to procedure or scope as an objection to accountability for a party widely blamed for the deaths of protesters in 2024. That framing made it politically costly for any member of parliament to press for slower deliberation, since doing so risked being read as defending the banned party rather than defending legislative process. Critics argue this is precisely how the Awami League ban became a vehicle for a much broader and more durable expansion of executive power over political speech, one that is no longer limited to the party that occasioned it.

[Taken together, these amendments reveal a pattern that goes well beyond banning a single organisation.](#) The government can now suspend a party's activities across nearly every sphere of political life without a prior judicial finding that it meets the legal threshold for terrorism. It can extend that suspension from the organisation's formal existence into everything its members do. It can silence the organisation's speech entirely, blocking its statements, its media presence, its rallies, and its public gatherings. At each stage, the decision rests with the government alone, with no independent court required to test whether the label of terrorism is deserved before the consequences take effect. What is presented as a security measure therefore functions, in practice, as [a mechanism that could just as easily be turned against any future political opposition, not only the one it was designed for.](#)

The Cyber Security (Amendment) Act, 2026: An Analysis

On 8 June 2026, Home Minister Salahuddin Ahmed told parliament that [the government had begun amending the Cyber Security Act, responding to a question from reserved-seat MP Helen Zerin Khan](#). He said the amendments were needed to enable the swift removal of harmful and defamatory AI-generated content from social media platforms, and that international platforms such as Meta would be required to remove disputed content within a set timeframe. He also alleged that defamatory content targeting the prime minister and his family was spreading under what he called the guise of freedom of expression, a framing that positioned the bill partly as protection for the ruling family specifically rather than the public at large.

What appears, at first glance, to be a narrow technical fix aimed at AI-generated deepfakes masks a familiar reality underneath. Beneath the surface justification of platform accountability lies a law that continues an enforcement architecture the government has never actually dismantled: content blocking and data requests carried out by administrative bodies rather than courts, built on definitional language broad enough to be stretched well past its stated purpose. This is not simply about defamatory deepfakes; it is about the sixth iteration of a cybercrime regime that has, in every prior version, [been used against journalists and dissenters far more often than against the harm it was introduced to solve](#).

The amendment operates on three fronts. First, it imposes platform takedown mandates, requiring international platforms named explicitly, including Meta, to remove disputed content within a specified timeframe. Second, it redefines misinformation and defamation in statute and raises the penalties attached to both. Third, it expands state power over data and content by authorising the Bangladesh Telecommunication Regulatory Commission and other authorised agencies to block content and to request user data directly from platforms, without disclosed statistics or a built-in judicial review requirement. [A separate cabinet committee, headed again by ICT Minister Fakir Mahbub Anam and including the Home, Foreign, Information and Law ministers, was formed on 2 July 2026 to finalise a related draft, described in official reporting as the Cyber Protection \(Amendment\) Act, 2026](#). Public reporting has not clarified whether this is a distinct instrument or an alternate rendering of the same law, a naming inconsistency that runs through coverage of the entire lineage of this legislation.

[Legal and press freedom commentary argues the combined effect of these three fronts is a continuation, not a correction](#), of a structure that has defined this area of law since 2006: executive and administrative content-blocking power without disclosed statistics or judicial oversight, paired with vague definitional language, including terms such as national unity, public order and content that creates anxiety, which gives enforcement discretion to police and bureaucrats rather than courts. [Commentary on the 2025 ordinance that preceded this amendment made the structural critique explicit](#), noting that content blocking on grounds like national unity or religious values carries no disclosure of blocking statistics, no judicial review requirement and no obligation to explain a decision, a structure the 2026 amendment does not appear to have altered. Because the amendment is framed around AI-generated content and platform accountability rather than the political speech provisions that drew the most criticism in

earlier versions, it has been easier for the government to present as a narrow technical fix, even though the underlying enforcement architecture remains unchanged.

Within about three weeks of passage, the amended law was already being used against journalists. On 22 June 2026, police charged six journalists from the daily Agradatra Pratidin under the Cyber Security Act 2026, alongside charges of criminal defamation, extortion and criminal intimidation, over their reporting on alleged corruption by a state minister for local government. [The Committee to Protect Journalists called for the charges to be dropped](#). Just before passage, on 3 June 2026, [CPJ's ten-point report on Bangladesh press freedom had specifically flagged what it called the Cyber Protection Act, 2026](#), warning that it retained vague provisions and weak oversight mechanisms found in prior cybercrime legislation used to restrict the press, a warning made while the bill was still moving through committee.

Timeline: From the ICT Act to the 2026 Amendment

- 2006: The Information and Communication Technology Act is enacted, with Section 57 criminalising fake, obscene or defamatory electronic content.
- 2018: [The Digital Security Act replaces the ICT Act's Section 57 regime](#). Over the following four years, more than 7,001 cases are filed under it, with only about two percent resolved in court and roughly sixty percent stemming from Facebook activity, overwhelmingly targeting journalists, opposition politicians and dissenters.
- August 2023: Facing sustained domestic and international pressure, [including a call from the United Nations High Commissioner for Human Rights to scrap the Digital Security Act, the Hasina cabinet approves the Cyber Security Act, reducing some penalties and making some offences bailable](#).
- 2024: [Amnesty International's Repackaging Repression briefing finds the Cyber Security Act rehashed almost all of the Digital Security Act's repressive provisions, and the law continues to be used against dissidents through the 2024 quota reform protests](#).
- 21 to 22 May 2025: The interim government repeals the Cyber Security Act and replaces it with an ordinance, dropping nine contentious provisions, including ones restricting criticism of the Liberation War, national leaders and constitutional institutions, though [a Clooney Foundation review finds vaguely worded provisions](#), including one criminalising content related to any religion or communal hate speech that creates anxiety, remain in place.
- 8 June 2026: [Home Minister Salahuddin Ahmed announces the government is amending the Cyber Security Act to target AI-generated defamatory content](#).
- 27 June 2026: [The Cyber Security \(Amendment\) Bill, 2026 is tabled and sent to committee](#).

- 30 June 2026: [The bill passes by voice vote after an opposition motion for public consultation is rejected.](#)
- 2 July 2026: [A cabinet committee is formed to finalise a related draft described as the Cyber Protection \(Amendment\) Act, 2026.](#)

Ministers presented the amendment as modernisation rather than restriction. [ICT Minister Fakir Mahbub Anam, who moved the bill in parliament, argued that other countries already require platforms to take down harmful content within twenty-four hours](#), and framed the amendment as bringing Bangladesh in line with that practice. The stated targets were AI-generated deepfakes and defamatory material, and the bill updated the statutory definitions of misinformation and defamation while raising penalties for violations, alongside empowering the Bangladesh Telecommunication Regulatory Commission and other authorised agencies to block content and request user data from platforms.

[The Cyber Security \(Amendment\) Bill, 2026 was tabled on 27 June 2026](#) and sent to the parliamentary Standing Committee on Law, Justice and Parliamentary Affairs with only a three-day turnaround for its report. [It passed by voice vote on 30 June 2026.](#) Jamaat-e-Islami members Shahjahan Chowdhury, M Abdul Gafur, Zahirul Islam, GM Nazrul Islam and Amir Hamza, along with independent MPs Rumeen Farhana and Sheikh Mujibur Rahman Iqbal, moved to send the bill back for public consultation. The motion was rejected by voice vote, and the bill proceeded on the same compressed timeline that had characterised the Anti-Terrorism Amendment two months earlier.

The bill moved quickly for reasons similar to those behind that earlier amendment. It was framed as narrowly targeting a novel problem, AI-generated deepfakes and defamation, rather than as a rewrite of the underlying cybercrime regime, which made it easier to present as urgent and uncontroversial. It also followed a now-familiar pattern in which each successive version of this law, the Digital Security Act, the Cyber Security Act, the 2025 ordinance and the 2026 amendment, has been justified as ending the misuse of the version before it, while retaining the same vague definitions and the same administrative blocking power. That repetition appears to have lowered the perceived stakes of any single amendment in the eyes of the government, even as the law's practical use against journalists, illustrated by the Agrajatra Pratidin case, continued uninterrupted across the transition from ordinance to statute and from one elected government to another.

The Committee to Protect Journalists has been the most active documented critic of the 2026 amendment specifically, both in [its pre-passage warning about vague provisions and weak oversight](#), and in [its subsequent call for the Agrajatra Pratidin charges to be dropped](#). [Its broader June 2026 report on Bangladesh found that more than 130 journalists had faced legal proceedings since the 2024 political transition](#), including charges as serious as murder and crimes against humanity, with at least five detained, and argued that the persistence of such cases under an elected government made continued use of these laws a political choice rather than an inherited legal accident. Transparency International Bangladesh has taken a similar position, arguing that a government which keeps unjust laws in place effectively endorses them, and [restating at its May](#)

[2026 World Press Freedom Day event](#) that the Information and Communication Technology Act, Digital Security Act and Cyber Security Act lineage should be repealed outright and replaced with legislation meeting international standards, rather than amended incrementally. In March 2026, [the Committee to Protect Journalists and eight other rights organisations wrote directly to newly elected Prime Minister Tarique Rahman urging his government to review cybercrime law cases against journalists and implement Media Reform Commission recommendations](#), a letter that predates the June amendment and appears to have gone unheeded on the cyber law front. [Amnesty International's earlier assessment of the 2025 ordinance had already flagged that broadly worded provisions](#), including undefined terms such as obscene video and vaguely defined cyber terrorism, remained a central concern even after the Digital Security Act's formal repeal.

Taken together, these amendments reveal a pattern that goes well beyond stopping AI-generated defamation. The government can now compel international platforms to remove disputed content on a fixed timetable, block content and request user data through administrative agencies rather than courts, and enforce definitions of misinformation and defamation broad enough to sweep in legitimate reporting. At each stage, the decision rests with regulators and police rather than an independent judicial process, and the law's use against six journalists within three weeks of passage suggests this is not a hypothetical risk. What is presented as a modernising, narrowly targeted fix therefore functions, critics warn, as the latest instalment in a twenty-year lineage of cybercrime law that has consistently been used against the press and political dissent, regardless of which government is in power or what the law is called at any given moment.