How Jailing People for Speech Destroys Democracy

Bangladesh's Proposed Cyber Security (Amendment) Act, 2027:

Problems and Remedies

(A historical review based on peer-reviewed journal research)

How defamation, sedition and "fake news" laws harm democracy once they turn into criminal punishment, and why speech offenses should carry fines only

Research report
Musa Ibne Mannan
PhD Researcher, UT Dallas, Texas, United States
(Author of 26 books published in Bangladesh and India under the pen name "Kishor Pasha Imon")
November 2026

A research paper drawing on peer-reviewed journal articles retrieved through the Eugene McDermott Library, The University of Texas at Dallas, and on legal texts, court decisions and current case reporting retrieved from the open web.

An "Aage Bangladesh" initiative (website: www.aagebangladesh.org)

Contents

Executive summary **1**
1. Scope, terms and method **3**
1.1 What counts as a “speech offense” here 3
1.2 “Felony-level” or criminal offenses 3
1.3 Sources and method 3
2. The historical record of escalation **4**
2.1 Medieval and early modern England: protecting the “magnates” 4
2.2 Colonial America and the early United States 4
2.3 Colonial India: sedition as a governing technology 4
2.4 The interwar period: democracies and dictatorships converge 5
2.5 Wartime America: the Espionage and Sedition Acts 5
2.6 Criminal libel that never left: the United States and Canada 5
2.7 The digital turn: cyber offenses raise the stakes 5
2.8 The “fake news” wave, 2018 to 2026 7
2.9 Summary of the escalation record 8
3. How escalation happens: recurring mechanisms **9**
3.1 Vague definitions transfer judgment to the enforcer 9
3.2 The penalty ratchet 9
3.3 The process is the punishment 9
3.4 Outsourced enforcement 9
3.5 Zombie laws and laws that change hands 9
4. The argument: speech offenses should never carry prison or felony status **10**
4.1 Design laws for the worst plausible government 10
4.2 In speech cases, the state is judging a dispute in which it is a party 10
4.3 The chilling effect (self-censorship) grows with the severity of the penalty 10
4.4 International human rights law already points this way 10
4.5 Civil and administrative remedies already exist 11
4.6 Prison does not fix the information problem 11
5. A fines-only model for defamation and misinformation **12**
5.1 Bangladesh’s proposed Cyber Security (Amendment) Act, 2027: problems and remedies 13
6. Counterarguments and responses **17**
6.1 Criminal libel mostly protects ordinary people 17
6.2 Reputation as dignity deserves criminal protection 17
6.3 Some falsehoods kill 17
6.4 Fines do not deter the powerful, and fines can also chill 17
6.5 Democracies with strong courts can be trusted 18
7. Summary of proposed changes **19**
8. Conclusion **21**
References **22**
Peer-reviewed articles 22
Legal instruments and court decisions 23
Reports and news sources for recent events 24

Executive summary

For more than seven centuries, governments have punished people for words said to be false, scandalous or harmful to the reputation of officials and the state. The labels have changed (scandalum magnatum, seditious libel, sedition, criminal defamation, “offensive messages,” “fake news,” “disinformation”), and the mechanism has stayed so much the same that it is instantly recognizable. It usually runs like this: a broadly worded offense is created, often for plausible reasons, in the name of public order or truth; it carries imprisonment; and it is then used most heavily against the critics of whoever holds power at the time.

This report traces that history from medieval England through the American Sedition Act of 1798, colonial India, the First World War, and the digital-era wave of cyber-libel and “fake news” laws in Bangladesh, India, the Philippines, Nigeria, Malaysia, Singapore, Hungary, Russia, Turkey and Pakistan. Across these cases, five recurring features of escalation appear: vague definitions; a ratchet in penalties (often when speech moves online); procedure used as punishment through arrest and denial of bail (an innocent person can easily spend weeks or months in jail, and even when released, the government pays no meaningful damages for the violation of their civil rights); enforcement outsourced to private complainants allied with power; and laws that survive the government that wrote them and pass into the hands of its rivals.

On that record, the report argues that speech offenses based on falsity, defamation or “misinformation” should never carry imprisonment or “criminal” or “felony” status. The core reason is institutional: a legislature writing a speech law should assume that the worst government it can imagine will one day enforce it.

A law that can only fine cannot be used to remove a journalist, opposition politician or activist from public life, and cannot be turned into indefinite pretrial detention. The report proposes a fines-only model with safeguards (income-scaled and capped fines, no imprisonment for non-payment, a truth and public-interest defense, an independent adjudicator, correction before penalty), and it keeps genuinely dangerous conduct such as true threats, incitement to imminent violence and fraud under the separate criminal laws that already cover it.

The report closes with the strongest counterarguments found in the peer-reviewed literature, including evidence that criminal libel in some jurisdictions is mostly used to protect private individuals from harassment, and arguments that fines alone may not deter wealthy or state-backed actors. Even so, the grave harm of taking a single second of a person’s liberty in state custody outweighs the harm of a hundred wealthy people spending money on disinformation and getting away with it.

1. Scope, terms and method

1.1 What counts as a “speech offense” here

The report covers criminal laws that punish expression on the ground that it is false, defamatory, insulting to officials or institutions, or likely to cause “panic,” “disorder” or damage to the “image” of the state. It groups them into four families:

- **Seditious libel and sedition:** criticism of the government or its officers treated as an offense against the state.
- **Criminal defamation and insult:** damage to the reputation of a person, often with heavier treatment for officials.
- **Cyber and “offensive message” provisions:** offenses tied to electronic communication, frequently copying defamation or public-order offenses with higher penalties.
- **False news, misinformation and disinformation offenses:** punishment for statements a court or official declares false and harmful to public order, health, security or the armed forces.

It does not argue for the abolition of laws against true threats, incitement to imminent violence, fraud, extortion, child sexual abuse material, or doxxing that facilitates stalking. Those offenses are defined by the harm or the act, and they can be enforced without asking a court to rule on whether an opinion about public affairs was “true.”

1.2 “Felony-level” or criminal offenses

“Felony” is a common-law category (crimes punishable by more than a year of imprisonment in the United States). Most of the countries discussed use other classifications, such as cognisable and non-bailable offenses in South Asian law or “grave” offenses in Russian law. The report therefore treats a speech offense as felony level when it carries imprisonment of more than one year, or when it permits arrest without warrant and detention without bail as of right.

(This paper also takes into account arrest of any length, not only felony-level offenses. If Bangladesh’s current draft cyber security law allows anyone to be arrested even for three days, or three hours, the ways in which that can gravely damage democracy are considered here as well.)

1.3 Sources and method

Peer-reviewed journal articles were located through the UT Dallas library discovery system (Primo, filtered to peer-reviewed content), searching on criminal defamation, seditious libel, sedition in India, fake news criminalization, the Bangladesh Digital Security Act, the Russian war “fakes” law, the Turkish disinformation law, the Nigerian Cybercrime Act, Philippine cyber-libel, COVID-era misinformation laws and chilling effects. Primary legal sources (UN Human Rights Committee General Comment No. 34, court judgments) and recent case reporting from news organizations and press-freedom NGOs fill in events that peer-reviewed literature has not yet covered, especially from 2023 to 2026. The reference list separates these categories so the reader can see which claims rest on peer-reviewed work.

One limitation matters for interpretation: much of the recent material is drawn from press-freedom organizations whose purpose is advocacy. Case counts from these groups are useful as orders of magnitude, and the report avoids relying on any single figure where sources disagree.

2. The historical record of escalation

2.1 Medieval and early modern England: protecting the “magnates”

The English statute of scandalum magnatum (1275) made it an offense to spread false news or tales about the great men of the realm. Lilienthal and Ahmad (2018) read the later law of sedition as a descendant of this idea: an offense designed less to prevent concrete harm than to shield the reputations and administrative methods of a ruling class from exposure. The Court of Star Chamber developed seditious libel in the early seventeenth century, and the doctrine passed to the common-law courts after Star Chamber was abolished. For most of this period, truth was no defense; a true criticism could be more dangerous to authority than a false one. Truth was only made admissible as a defense in English criminal libel by the Libel Act 1843.

Historians of the eighteenth century show how sweeping and dangerous the offense was. Hunt (2017) documents seditious libel prosecutions reaching even the servants and apprentices of the printers who published the offending text, people who had no real control over its content. In other words, once a law of this kind is on the books, it can destroy almost anyone’s life.

Rushton (2015) traces prosecutions for “seditious words” spoken in taverns and streets between 1650 and 1750. Page (2009) describes the Dean of St Asaph’s trial in the 1780s, in which the central fight was over whether the jury or the judge decided if a publication was criminal.

2.2 Colonial America and the early United States

Nelson (1959) shows that seditious libel (an offense much like the “belittling” or “dignity of the state” provisions of today’s Cyber Security Act) crossed the Atlantic with English law and was used by colonial authorities against printers. The independent United States then made such speech a crime again within a decade of ratifying the First Amendment (the guarantee of free speech that is now admired worldwide).

The Sedition Act of 1798, passed by a Federalist Congress during a war scare with France, made it a crime to publish “false, scandalous and malicious” writing against the government, Congress or the President. Jenkins (2001) argues that the Act and the controversy around it shaped how seditious libel was first absorbed into, and later rejected by, First Amendment doctrine. Without that rejection, America would not have the free speech it has today. Notably, First Amendment doctrine had to consider, and accept, that people (those with good intentions and bad alike) must be left free even to speak scandalously, or there would be no free speech at all.

The enforcement pattern is instructive. The first person tried was Matthew Lyon, a sitting opposition congressman from Vermont, who was fined $1,000 and sentenced to four months in jail, and who could not be released at the end of the term until the fine was paid. James Callender, a Republican pamphleteer, received nine months and a $200 fine. Wendell Bird’s archival study of the prosecutions, reviewed in several peer-reviewed history journals (Mayeux, 2021; Kanstroom, 2020; Rakove, 2022), found considerably more prosecutions than the traditional count, almost all of them against supporters of the opposition Democratic-Republican party.

The Act expired in March 1801, on the last day of the administration that had enacted it, and it is now widely regarded as a constitutional embarrassment. The law worked exactly as its critics predicted: as a tool for an incumbent party facing an election.

2.3 Colonial India: sedition as a governing technology

Section 124A was added to the Indian Penal Code in 1870 and became the colonial government’s main instrument against the nationalist press. Lilienthal and Ahmad (2018) describe it as a provision devised primarily to oppress, and Yadav (2023) traces its ambiguous wording, its survival after independence, and comparative developments in the United Kingdom and the United States. Leonard (2024) shows that the

same eighteenth-century English seditious libel precedents continued to frame Indian free-speech adjudication until the 1950s. The provision survived independence and was upheld, with a narrowing interpretation, in Kedar Nath Singh v. State of Bihar (1962).

Its later history illustrates how hard such laws are to kill. In May 2022 the Supreme Court of India put Section 124A in abeyance in *S.G. Vombatkere v. Union of India*. When the Bharatiya Nyaya Sanhita replaced the Penal Code in July 2024, it dropped the word "sedition" but introduced Section 152 on acts endangering the sovereignty, unity and integrity of India, which petitioners have challenged as a repackaged sedition offense (Sonkar, 2026). That challenge was still pending at the time of writing.

2.4 The interwar period: democracies and dictatorships converge

Skinner (2016) compares the offense of "vilification" of the state in the 1930 Italian Fascist Penal Code with English seditious libel in the same period. He finds important common ground in the scope and purpose of the two offenses, and argues that a liberal democracy and a fascist state shared a similar conception of the state interest that speech law protects. The finding is uncomfortable and central to this report: speech crimes are not peculiar to dictatorships. Democracies build them too, and the instruments then remain within reach of whoever governs next, who use them freely against anyone they dislike.

2.5 Wartime America: the Espionage and Sedition Acts

During the First World War, the Espionage Act of 1917 and the Sedition Act of 1918 criminalized false statements interfering with the war effort and "disloyal" or "abusive" language about the government. Eugene Debs, the Socialist Party leader, was sentenced to ten years in federal prison for an anti-war speech in Canton, Ohio, in June 1918, and the Supreme Court unanimously upheld his conviction in 1919. He ran for president from his prison cell in 1920. Stone (2004) shows that the pressure to prosecute dissenters returned in the Second World War, when critics of the administration were labeled purveyors of falsehood, and draws the comparison with the prosecutions of 1798.

2.6 Criminal libel that never left: the United States and Canada

Lisby (2004) argues that criminal libel has no legitimate place in a democracy and that its continued existence is incompatible with the First Amendment's commitment to equality of speakers. Empirical work shows the offense did not disappear. Pritchard (2009) found that criminal libel was prosecuted in Wisconsin far more often than scholars assumed between 1991 and 2007. In Canada, Taylor and Pritchard (2018) identified more than 400 criminal libel prosecutions since 2000, a substantial share of which punished citizens' political speech, especially criticism of police and other justice officials. Their title captures a theme of this report: the process is the punishment.

2.7 The digital turn: cyber offenses raise the stakes

From the mid-2000s, many states wrote new offenses for electronic communication. These provisions often duplicated existing defamation or public-order crimes, then attached harsher penalties and looser procedural protections because the speech happened online.

Bangladesh: ICT Act, Digital Security Act, Cyber Security Act

Bangladesh offers the clearest example of a penalty ratchet. The Information and Communication Technology Act 2006, passed under a BNP-Jamaat government, carried a maximum of ten years for publishing false, obscene or defamatory electronic material. In 2013, under an Awami League government, Section 57 was amended to set a minimum of seven years and a maximum of fourteen, to make the offense non-bailable, and to allow arrest without warrant. The same defamatory statement in print attracted up to two years under the Penal Code. According to research by Ali Riaz for the Centre for Governance Studies,

1,417 cases were filed under the ICT Act between 2012 and June 2017, about 65 percent of them under Section 57.

Section 57 was repealed in 2018 and replaced by the Digital Security Act (DSA), which retained and expanded the speech offenses. Lacy and Mookherjee (2020) describe the ICT Act and DSA as "firing cannons to kill mosquitoes": the laws enabled powerful people, party loyalists and attention seekers to act as "digital vigilantes," and pending charges were left suspended so they could be revived later, producing fear as an environment. Bhowmik and Fisher (2026), interviewing fifteen digital journalists, found that the DSA produced fear of jail and even disappearance and pushed reporters into "defensive journalism." Zafarullah and Nughat (2026) document how the law fed self-censorship among ordinary social media users.

The human cost became visible in the case of the writer Mushtaq Ahmed, arrested in May 2020 over Facebook posts criticizing the government's pandemic response. He was denied bail six times and died in Kashimpur prison on February 25, 2021 after about ten months in pretrial detention. He was never convicted. Transparency International Bangladesh reported 197 DSA cases against 457 people in 2020 alone.

The DSA was replaced by the Cyber Security Act 2023, and after the political transition of 2024 by the Cyber Security Ordinance 2025, gazetted in May 2025. The Ordinance repealed nine contentious sections that the law adviser said accounted for about 95 percent of cases (including defamation, "false" or "offensive" information, and offenses relating to the Liberation War and the Father of the Nation), ordered pending cases under them dismissed, and made the remaining speech-related offenses bailable. Commentators note that it still keeps imprisonment for some expression offenses and broad state powers over content. The sequence matters for this report's argument: the same legal architecture was written by one party, intensified by its rival, and dismantled only after a change of government.

India: Section 66A of the IT Act

Section 66A of India's Information Technology Act punished "grossly offensive" or "menacing" messages and false information sent to cause "annoyance" or "inconvenience," with up to three years in prison. The Supreme Court struck it down as unconstitutionally vague in Shreya Singhal v. Union of India (2015). Police kept using it. In petitions to the Court, the People's Union for Civil Liberties reported 1,307 cases registered in eleven states after the judgment, and the Court did not order all pending 66A cases closed until October 2022. A speech offense can therefore outlive its own invalidation by seven years. Mittal (2016) examines what Shreya Singhal implied for the sedition provision.

The Philippines: cyber-libel

The Cybercrime Prevention Act of 2012 extended criminal libel to online publication and raised the penalty by one degree. Abcede and Robie (2015) describe journalists' comparison of the law to "e-martial law," recalling the Marcos-era suppression of the press. In June 2020, the journalist and later Nobel Peace Prize laureate Maria Ressa and former researcher Reynaldo Santos Jr. were convicted of cyber-libel over a 2012 article, under a law passed after the article was first published. The Court of Appeals affirmed the conviction in 2022 and lengthened the maximum sentence to more than six years; the latest reports found for this review describe the Supreme Court appeal as still pending. In 2011 the UN Human Rights Committee had already found, in Adonis v. Philippines, that imprisoning a broadcaster for libel violated Article 19 of the ICCPR.

Nigeria: the Cybercrime Act

Section 24 of Nigeria's Cybercrime Act 2015 criminalized "cyberstalking," including messages known to be false and sent to cause "annoyance" or "insult." Adibe, Ike and Udeogu (2017) show that Nigeria's online press-freedom ranking worsened after the Act and attribute this to its use against journalists by political leaders. In March 2022 the ECOWAS Court of Justice found Section 24 arbitrary, vague and repressive and ordered Nigeria to repeal or amend it. A 2024 amendment rewrote the section, but civil society litigants

argue the new version, which still criminalizes messages likely to cause a “breakdown of law and order,” reproduces the problem.

2.8 The “fake news” wave, 2018 to 2026

After 2016, “fake news” became a global political vocabulary, and a new generation of laws criminalized falsity itself, usually without any requirement that a particular person be defamed.

- **Malaysia (2018).** The Anti-Fake News Act entered into force in April 2018, weeks before a general election, with penalties of up to six years and RM500,000. The first person convicted was a Danish visitor who posted a video criticizing police response times; he was sentenced to a week in jail plus a fine and, saying he could not pay, faced a default term of a month. The government that passed the law lost the election, and its successor moved to repeal it within months.
- **Singapore (2019).** The Protection from Online Falsehoods and Manipulation Act (POFMA) relies mainly on ministerial “correction directions,” but Section 7 makes knowingly communicating a harmful false statement of fact a crime punishable by up to five years, and up to ten in aggravated cases. Its first criminal prosecution under Section 7 was brought in March 2026 against a government critic. Teo and Kiu (2021) analyze conflicting early High Court decisions on who bears the burden of proving a statement false on appeal.
- **Hungary (2020).** On March 30, 2020, emergency COVID-19 legislation expanded the crime of “scaremongering” and allowed up to five years in prison for false or distorted statements that hinder the pandemic response. Police opened 86 investigations within weeks, including detentions over critical Facebook posts.
- **Russia (2022).** Article 207.3 of the Criminal Code, adopted on March 4, 2022, punishes “knowingly false information” about the use of the armed forces with up to fifteen years. The Moscow municipal councillor Alexei Gorinov received seven years for remarks at a council meeting about children dying in Ukraine. Sherstoboeva (2024), analyzing 446 court decisions from 2022 and 2023, shows that courts treated any deviation from official Defense Ministry statements as false, so that truth became conditional on loyalty. Court statistics compiled by independent media counted 82 sentences under the article in 2024.
- **Turkey (2022).** Law No. 7418 added Article 217/A to the Penal Code, punishing public dissemination of “misleading information” with one to three years. Yücel (2025) places it within a model of “hybrid digital authoritarianism.” The first journalist convicted, Sinan Aygül, received ten months for a post he had already corrected; the Court of Cassation overturned the conviction in 2024. Prosecutions continued, with Istanbul courts in April 2026 imposing sentences of up to two and a half years on journalists for televised commentary.
- **Indonesia (2023).** The new Penal Code retained offenses for broadcasting fake news that disturbs public order. Prahassacitta and Harkrisnowo (2024) analyze its justification and limits, while Aryana and colleagues (2026) document more than 530 criminalization cases under the Electronic Information and Transactions Law between 2019 and 2024 and survey evidence of self-censorship.
- **Pakistan (2025).** The Prevention of Electronic Crimes (Amendment) Act 2025 added Section 26(A), punishing intentional dissemination of information known or believed to be false and likely to cause “fear, panic or disorder” with up to three years and a fine of Rs2 million. It passed both houses within about a week of introduction.

Pomeranz and Schwid (2021), reviewing governmental responses to COVID-19 misinformation worldwide, found that criminalizing expression was one of five main categories of state action, alongside the more troubling category of governments themselves restricting accurate information and spreading false

information. Vese (2022) warns that health emergencies offer a pretext for draconian restrictions on expression.

2.9 Summary of the escalation record

Period / place	Law	Maximum custodial penalty	Pattern observed
England, 1275 onward	Scandalum magnatum; seditious libel	Imprisonment, pillory; truth no defense until 1843	Protects officials from criticism
United States, 1798	Sedition Act	Up to 2 years and fine	Incumbent party prosecutes opposition editors and a congressman
British India, 1870	Penal Code s.124A	Up to life imprisonment	Colonial tool kept after independence; renamed in 2024
United States, 1917–18	Espionage and Sedition Acts	Up to 20 years	Anti-war speakers jailed; Debs given 10 years
Bangladesh, 2006–2023	ICT Act s.57; DSA; CSA	14 years (2013), non-bailable	Penalty ratchet; death in pretrial custody
India, 2009–2015	IT Act s.66A	3 years	1,307 cases after the law was struck down
Philippines, 2012	Cybercrime Prevention Act	Libel penalty raised one degree	Nobel laureate journalist convicted
Malaysia, 2018	Anti-Fake News Act	6 years	Passed before an election; repealed after it
Hungary, 2020	Scaremongering (emergency law)	5 years	Pandemic used to criminalize criticism
Russia, 2022	Criminal Code art. 207.3	15 years	Truth defined by the Defense Ministry
Turkey, 2022	Penal Code art. 217/A	3 years	Journalists prosecuted for corrected or contested reports
Pakistan, 2025	PECA s.26(A)	3 years	Rushed passage; vague “panic” standard

Table 1. Selected speech offenses carrying imprisonment. Penalties are statutory maxima as reported in the sources cited in Section 2.

3. How escalation happens: recurring mechanisms

3.1 Vague definitions transfer judgment to the enforcer

Words such as “false,” “misleading,” “offensive,” “tarnishing the image of the state” and “causing panic” have no stable legal meaning. Courts struck down Indian Section 66A, Nigerian Section 24 and Kenyan criminal defamation in part on this ground. Vagueness matters more as penalties rise, because the person deciding what counts as “false” now controls whether someone loses years of liberty. In Turkey, journalists prosecuted under Article 217/A report that authorities often fail to say which part of a report is misleading.

3.2 The penalty ratchet

Speech offenses rarely stay at their starting level. Bangladesh moved from ten years to fourteen with a seven-year minimum. The Philippines added a degree to libel once it was online. Pakistan’s 2025 draft initially proposed seven years before settling on three. Each new medium (print, broadcast, internet, social media, now generative AI) is treated as uniquely dangerous and earns a harsher rule, while the older offenses remain on the books. The result is that the same sentence can carry two years in a newspaper and fourteen on Facebook.

3.3 The process is the punishment

Imprisonment as a sentence is only part of the risk. Non-bailable status, arrest without warrant and long pretrial detention allow the state to impose months of custody without any conviction. Mushtaq Ahmed died without a verdict. Taylor and Pritchard (2018) show that in Canada the arrest, charge and long trial process punished critics of police even when convictions did not follow. Lacy and Mookherjee (2020) note that in Bangladesh charges were often left suspended so they could be reactivated later, keeping the accused under permanent threat. Any speech offense that permits detention carries this risk, however rarely it ends in a conviction.

3.4 Outsourced enforcement

Many digital speech laws allow any person to file a complaint. In Bangladesh, Ali Riaz reported in 2023 that about 39 percent of the DSA cases his team studied were filed by individuals affiliated with the then ruling party, and Lacy and Mookherjee (2020) describe a class of “digital vigilantes” who use the law to settle personal and political scores. This multiplies prosecutions beyond anything a central government would direct, while giving the government deniability.

3.5 Zombie laws and laws that change hands

Speech offenses persist after courts invalidate them (India’s Section 66A), after governments promise to review them (Section 124A becoming Section 152), and after their authors fall from power. Bangladesh’s ICT Act was written under one government and turned into a fourteen-year non-bailable offense by its rival. Malaysia’s Anti-Fake News Act was passed to protect a government that lost the election weeks later. The American Sedition Act of 1798 was enacted by Federalists who would themselves have been exposed to it under a Republican administration had it not expired. A legislator who supports a speech crime because “our side” will enforce it responsibly is betting against this history.

4. The argument: speech offenses should never carry prison or felony status

4.1 Design laws for the worst plausible government

The central argument is institutional. A law is a tool that outlasts the people who write it. When a legislature decides whether false or defamatory speech may be punished with prison, it is choosing what power to hand to every future government, including governments it would regard as illegitimate, corrupt or authoritarian. The historical record above shows that this transfer happens in practice: incumbents facing elections (1798, Malaysia 2018), governments in emergencies (Hungary 2020), governments at war (the United States 1918, Russia 2022), and governments consolidating power (Bangladesh 2013 to 2023, Turkey 2022) have all reached for the custodial speech offense they found on the statute book or could quickly create.

Under this test, legislators should ask how much damage the law could do in the hands of the worst government plausibly able to win power. Imprisonment fails that test because it is the one sanction that physically removes a critic from public life, can be imposed before trial, and can be extended to end a career or a life. A fine, however large, leaves the speaker free to speak again, to appeal, to organize, and to vote.

4.2 In speech cases, the state is judging a dispute in which it is a party

Most false-news offenses ask a prosecutor, and then a court, to decide what is true about public affairs. When the subject is government performance, the state is both the accuser and the most interested party. Sherstoboeva (2024) shows the end point of this structure in Russia, where courts treated the Defense Ministry's account as the definition of truth. Turkish journalists describe the same dynamic, in which any information not sourced from the government is liable to be labeled false. Even in better-functioning systems, facts about pandemics, wars and economic policy are contested and change as evidence arrives. Statements labeled misinformation in one year can become mainstream later. Attaching years of imprisonment to a judgment this unstable is disproportionate on its face.

4.3 The chilling effect (self-censorship) grows with the severity of the penalty

Coenen (2012) argues that courts should be "penalty-sensitive" in free-speech cases, because the severity of a sanction changes how much protected expression a rule deters. A rule that is tolerable as a modest fine can be unconstitutional as a prison term. The empirical work supports this. Bhowmik and Fisher (2026) found that the fear of jail, and not merely of liability, reshaped Bangladeshi journalism. Aryana and colleagues (2026) describe cascading chilling effects in Indonesia that extend far beyond the individuals prosecuted. Because most people cannot predict how a vague rule will be applied, they respond to the worst outcome, and imprisonment makes the worst outcome catastrophic.

4.4 International human rights law already points this way

The UN Human Rights Committee's General Comment No. 34 (2011), the authoritative interpretation of Article 19 of the ICCPR, states at paragraph 47 that states should consider decriminalizing defamation, that criminal law should be applied only in the most serious cases, and that imprisonment is never an appropriate penalty. The Committee applied that standard in Adonis v. Philippines (2011). Regional courts have followed. Shelton (2015) explains how the African Court on Human and Peoples' Rights, in Konaté v. Burkina Faso (2014), held that imprisoning a journalist for defamation violated the African Charter, applying necessity and proportionality rather than deferring to national "clawback" clauses. The Zimbabwe Constitutional Court (Madanhire, 2014), the High Court of Kenya (Okuta, 2017) and the Lesotho Constitutional Court (Peta, 2018) struck down criminal defamation altogether, and the ECOWAS Court condemned Nigeria's cyberstalking provision (2022). Spaic, Nolasco and Novovic (2016) trace a similar, if uneven, decriminalization movement among EU and Balkan states.

This report goes one step further than General Comment No. 34, which still allows criminal defamation in "the most serious of cases." It argues that the same logic that rules out imprisonment for defamation also rules it out for false-news and misinformation offenses, which are vaguer and more political than defamation because they lack an identifiable victim.

4.5 Civil and administrative remedies already exist

The courts in Zimbabwe, Kenya and Lesotho reasoned that criminal defamation is unnecessary because a person whose reputation is harmed can sue for damages. The same applies to most misinformation: the state can publish corrections, require platforms to label or reduce the reach of content, and fund independent fact-checking. Pomeranz and Schwid (2021) conclude that public health is best served by protecting expression, disseminating accurate information, protecting whistleblowers and supporting independent media, and that governments undermine public health when they create uncertainty and violate rights. Marecos and colleagues (2023) similarly find that speech-restrictive solutions to health misinformation run into serious constitutional and ethical limits and favor media literacy, fact-checking and credibility signals. Anansaringkarn and Neo (2021), studying Thailand, argue that equating fake news with illegality undermines liberties and recommend transparency obligations on technology companies first.

4.6 Prison does not fix the information problem

There is little evidence that imprisoning individual speakers reduces misinformation at scale. Large-scale disinformation is mostly produced by coordinated networks, commercial operations and, often, states themselves. Pomeranz and Schwid (2021) list governments disseminating false information as a category of COVID-19 response in its own right. Criminal false-news laws are almost never used against governments' own falsehoods. They are used against individuals at the edge of the network: a Danish visitor, a councillor, a cartoonist, a local journalist. Prison removes the critic and leaves the falsehood in circulation.

5. A fines-only model for defamation and misinformation

Accepting that some regulation of harmful falsehood is legitimate, the proposal is that the maximum sanction for any expression-based offense of falsity, defamation or "misinformation" should be a monetary penalty, imposed through a civil or administrative process, with no criminal record and no possibility of custody. The model has the following elements.

Sanction design

1. **No imprisonment, ever, including for non-payment.** History shows fines turning into jail when the speaker cannot pay: Matthew Lyon stayed in jail until his fine was paid in 1798, and the Danish defendant in Malaysia faced a month in jail for the same reason. Unpaid penalties should be recoverable only as civil debts.
2. **Income-scaled and capped fines.** A flat fine is trivial for a wealthy actor and ruinous for a student or a freelance journalist. A day-fine model (a number of days of income, with a hard ceiling for individuals) keeps deterrence proportionate and prevents the fine from becoming a back-door means of destroying critics.
3. **Higher, separate penalties for organizations and coordinated operations.** Commercial disinformation services, bot networks and platforms that fail to meet transparency duties can face larger administrative fines, keeping the heaviest burden on actors with scale rather than on individual speakers.

Procedure

1. **No arrest, detention or seizure of devices** in any proceeding on these grounds. Proceedings begin by written notice.
2. **Correction and right of reply before any penalty.** The first remedy should be a published correction or reply, which addresses the harm directly. A penalty should follow only if a speaker who knew the statement was false refuses to correct it.
3. **Burden on the state or claimant to prove falsity, knowledge and harm.** Opinion, satire and statements on matters of public interest made in good faith are protected. Teo and Kiu (2021) show how much turns on where this burden is placed.
4. **An independent adjudicator.** Decisions on falsity should be made by an independent court or tribunal, never by a minister or an agency answering to the government whose conduct is being discussed.
5. **No private criminal complaints.** Individuals harmed by defamation keep their civil claim; they cannot trigger state enforcement for others' speech about public affairs.

Safeguards against drift

1. **Statutory ceiling in the constitution or a supermajority statute.** Because the risk is a future government raising penalties, the no-imprisonment rule should be entrenched against ordinary amendment.
2. **Transparency reporting.** Annual publication of every proceeding, the speaker's profession, the complainant's identity where an official, and the outcome, so misuse against journalists and opposition figures is visible.
3. **Sunset and review clauses** on any emergency speech measure, as the Hungarian opposition sought, unsuccessfully, in 2020.

What stays criminal

This model leaves untouched the criminal law of true threats, incitement to imminent violence, fraud, extortion, perjury, impersonation for financial gain, and sexual abuse imagery. Those offenses are defined by an act or an imminent harm, not by a disputed claim about public affairs. Where a false statement is a component of such an offense (for example, a fake emergency report to police, or a fraudulent investment

pitch), prosecutors should charge the underlying offense. Conduct that is already criminal for other reasons stays criminal; the model only removes "falsity" and "reputation" as independent grounds for prison.

5.1 Bangladesh's proposed Cyber Security (Amendment) Act, 2027: problems and remedies

The earlier draft of this report did not discuss the proposed amendments to the Cyber Security Act, 2026 (Act No. 81 of 2026), and it left out their religious dimension. This section fills that gap. The analysis is based on the comparative statement titled "Proposed Amendments to the Cyber Security Act, 2026" (the version without comments, dated November 9, 2026), which sets the current law and the proposed "Cyber Security (Amendment) Act-2027" side by side. The draft is not final, so its wording may change before it reaches Parliament. Each problem is set out separately below, together with proposals on what should and should not be done.

A. The religious dimension: an effective blasphemy provision without the name (Sections 26, 26A and 8(2)(b))

The problem. Nowhere does the draft expressly mention "insulting" the Prophet Muhammad or any other religious figure. Yet read together, three provisions amount in practice to a blasphemy law, and those most at risk will be atheists, skeptics and critics of religion.

First, the current Section 26(1) criminalizes any publication that is "religious or communal hate speech" and that causes violence "or creates anxiety." "Anxiety" is so low a threshold that it is met as soon as anyone is upset by a criticism of religion. The law draws no distinction between criticizing religious ideas, scriptures or religious figures and spreading hatred against the people of a community. A critical essay about the Prophet's life or conduct could therefore easily be alleged to be "religious hate speech," and the reaction of an angry crowd would itself become the proof of "creating anxiety."

Second, the draft raises the maximum sentence under Section 26(2) from 2 years to 5 years, and amends Section 46(2) to make Section 26 offenses non-bailable instead of bailable. The 2025 Ordinance had made speech offenses bailable; this draft reverses that reform. It is a direct example of the upward penalty pressure described in Section 3.2.

Third, the new Section 26A provides up to 5 years' imprisonment for spreading "rumors and disinformation," and this too is non-bailable. The explanation to the definition of "rumor" uses, as its example, a campaign that inflames religious sentiment. This opens the way for questioning the truth of religious narratives or historical claims to be charged as "false or distorted information," and in effect puts the courts in the position of deciding religious truth.

Fourth, under Section 8(2)(b), the mere "apprehension" of religious or communal violence is enough for law enforcement, the Ministry of Information and Broadcasting, or any agency empowered by the government to remove or block content.

This structure is not new. Section 57 of the ICT Act as amended in 2013 made "hurting religious sentiment" an offense, and in 2013 several bloggers, including Asif Mohiuddin, Mashiur Rahman Biplob, Subrata Adhikari Shuvo and Russell Parvez, were arrested in ICT Act cases. The proposed Section 26 would do the same job as that provision, only without using the words "religious sentiment." Under paragraph 48 of the UN Human Rights Committee's General Comment No. 34, prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the ICCPR, except in the circumstances of incitement to violence, hostility or discrimination covered by Article 20(2).

What should be done

Limit the scope of Section 26 so that only speech that incites violence, hostility or discrimination against the members of a religious or ethnic group is an offense, where intent to incite is proved and there is a real

likelihood of imminent harm. Write into the text of the law the six criteria of the UN Rabat Plan of Action (2012): context, the speaker's position, intent, content and form, extent of dissemination, and likelihood and imminence of harm.

Add an explicit safeguard clause: criticism, satire, and historical or academic analysis of religion, scripture, the Prophet or other religious figures and religious institutions, as well as the expression of apostasy or unbelief, shall not be an offense under this Act.

Remove the words "creating anxiety" and "apprehension" from Sections 26 and 8(2)(b).

Place criminal liability on those who mobilize crowds to violence in reaction to a piece of writing. The original author's liability should be limited to their own words; someone else's violent reaction must not become proof of the author's offense.

Apply this report's fines-only model to hateful speech that does not reach the level of incitement.

What should not be done

Add any wording such as "hurting religious sentiment," "insulting religion," "derogatory remarks" or insulting the Prophets to the law, or accept such an amendment if it is raised during parliamentary debate.

Accept listeners' outrage, processions or the volume of online protest as proof of an offense.

Make Section 26 non-bailable or raise its sentence to 5 years.

Give a court or any government agency the task of deciding whether religious claims are true or false.

B. Rumors and disinformation (Sections 2(aa), 2(jj) and new Section 26A)

The problem. The 2025 Ordinance repealed the offense of publishing "false" and "offensive" information. The draft brings that class of offense back under a new name, this time with up to 5 years' imprisonment or a fine of Tk 10 lakh, and as a non-bailable offense. The explanation to the definition of "disinformation" lists "damaging the image of the state" as an element of harm, reviving the much-criticized "image of the state" concept of the DSA. The first step in deciding what is false lies with the police and the ministry. The experience of Malaysia, Russia and Turkey described in Section 2.8 shows that provisions of this kind are used most against journalists and critics of the government.

What should be done. An order to publish a correction as the first remedy; income-scaled fines only where knowingly false publication, refusal to correct and actual harm are all three proved; adjudication by an independent tribunal; an explicit exemption for information published in good faith and later corrected. Remove words such as "image of the state" from the definitions and explanations.

What should not be done. Keep imprisonment or non-bailability; treat disagreement with a government statement as proof of falsity; make the "apprehension" of harm a basis for punishment.

C. Cyber defamation (new Section 25A)

The problem. The 2025 Ordinance repealed the offense of defamation by publication because it was the one most used against journalists. The draft adds it back in Section 25A, with up to 2 years' imprisonment or a fine of Tk 5 lakh. Criminal defamation already exists under Sections 499 and 500 of the Penal Code, so this opens two separate criminal routes for the same statement.

What should be done. Limit defamation to civil remedies; at most, fines with defenses of truth, opinion and public interest; the right to file a complaint only for the person directly aggrieved.

What should not be done. Keep imprisonment; create a second criminal defamation offense alongside the Penal Code; allow third parties to bring cases on someone else's behalf.

D. Belittling and bullying (Sections 2(rr), 2(ff) and new Section 25B)

The problem. The definition of "belittling" (heyoprotipanno) criminalizes injuring someone's self-respect with the intent of contempt, ridicule or scorn, and the explanation expressly mentions creating caricatures or memes by editing photos or videos. The penalty is up to 3 years' imprisonment, and the offense is non-bailable. The definition refers to "exceeding the limits of constructive criticism," but does not say who decides which criticism is constructive. This provision puts political cartoons, satire and parody directly at risk; the DSA case against the cartoonist Ahmed Kabir Kishore foreshadows how it will be used. Satire about religious figures can also be brought under this section.

What should be done. Keep a narrow provision to protect private individuals from harassment and bullying, where the conduct is repeated, targets a specific person and arises from an imbalance of power; the remedies should be protection orders and fines. Expressly exempt satire, parody and cartoons about public officials, public figures, institutions and religious figures.

What should not be done. Make ridicule or mockery a criminal offense; leave room for this section to be used to silence criticism of officials.

E. Powers to remove and block content (Sections 8(2), 8(3) and 8(4))

The problem. The draft extends the blocking power beyond law enforcement to the Ministry of Information and Broadcasting and to any agency empowered by the government. The list of grounds now adds the country's "dignity," defamation and belittling, and attaches the phrase "where there is apprehension" to each ground. Under the current law, a tribunal's approval must be obtained within 3 days of a block, and if it is not, the content must be restored; the draft removes this judicial oversight and tells the aggrieved person to appeal to the same agency. The obligation to publish a list of all blocked content has also been dropped.

What should be done. Keep the requirement of tribunal approval within 3 days and automatic restoration if approval is not given; maintain a public register of blocked content; appeals to go to an independent tribunal.

What should not be done. Give the Ministry of Information the power to block criticism of itself or of the government; keep vague grounds such as "dignity" or "apprehension."

F. Non-bailability, arrest, and protection only for registered media (Section 46 and new Section 46A)

The problem. Under the draft, offenses under Sections 25, 25B, 26 and 26A will be non-bailable. The new Section 46A requires the tribunal's prior permission before an arrest, but only for content published in registered media outlets. Bloggers, YouTubers, Facebook writers, independent writers and critics living abroad will not get this protection, even though the sharpest criticism of religion and politics usually comes from them. This turns freedom of speech into a privilege that depends on a license. The death of Mushtaq Ahmed (Section 2.7) shows how far the consequences of a non-bailable speech offense can go.

What should be done. No arrest for any speech offense, with proceedings begun by written notice; until that is achieved, at the very least extend the prior-permission protection of Section 46A to every person.

What should not be done. Divide citizens into two classes on the basis of registration or licensing; keep speech offenses non-bailable.

G. Canceling the registration and licenses of media organizations (Section 29(3))

The problem. If a company is convicted, the court may suspend or cancel its registration, license or operations, and registered media outlets fall within this. Although there is a 15-day notice requirement, it opens the way to shutting down an entire organization over a single statement, a punishment that would fall on all its staff and readers.

What should be done. Proportionate fines for organizations and orders to publish corrections.

What should not be done. Keep any provision for shutting down media outlets or canceling their licenses for speech offenses.

H. Composition of the Council, oversight and immunity for officials (Sections 12, 14 and new Section 52)

The problem. The Chairman of the National Human Rights Commission is being removed from the National Cyber Security Council, while the Home Minister, the Foreign Minister and the Minister of Information and Broadcasting are being added. The Council will meet once every 6 months instead of every 3 months. The new Section 52 gives Council members and all officials acting under the law immunity from civil and criminal proceedings for acts done "in good faith." Powers are growing while oversight and accountability are shrinking.

What should be done. Bring the Human Rights Commission back onto the Council and add independent representatives of journalists and civil society; publish an annual report listing every case, every block and the identity of each complainant; impose fines on those who file false or harassing complaints.

What should not be done. Grant blanket immunity to officials who misuse the law.

Overall assessment. Almost all of the five mechanisms described in Section 3 can be seen in this draft: vague words ("anxiety," "apprehension," "dignity," "belittling"); upward penalty pressure (2 to 5 years, bailable to non-bailable); room to use arrest and detention as punishment; executive control in place of judicial oversight; and the rebuilding of an architecture that was dismantled in 2025. Whichever government proposes the draft now, if it passes, these powers will pass to every future government.

6. Counterarguments and responses

A fair assessment requires engaging with the strongest objections in the literature.

6.1 Criminal libel mostly protects ordinary people

Pritchard (2009) found that most Wisconsin criminal libel cases had nothing to do with politics, that the First Amendment protected defendants in the rare political cases, and concluded that criminal libel can legitimately address harms to private individuals. Taylor and Pritchard (2018) likewise found many Canadian cases involved sexual slurs against former partners. Victims of this kind of abuse often cannot afford civil litigation, and the defendant may be judgment-proof.

Response. The harms in these cases are real, and they are better described as harassment, intimate-image abuse or stalking, which can be addressed by targeted offenses defined by the conduct, with protective orders. The same Canadian study found that a substantial share of prosecutions targeted criticism of police and justice officials, which shows how a general defamation offense drifts toward protecting officials. A narrowly drawn harassment offense protects private victims without giving the state a general power to imprison speakers over reputation.

6.2 Reputation as dignity deserves criminal protection

Anstey (2017) argues that much of the abolition literature fails to analyze reputation properly, and that in many legal cultures reputation is closer to honor or dignity, a personal interest the state may legitimately protect. Several European and Asian systems treat defamation primarily this way, as reflected in the Polish, Serbian and Croatian debates in the library results.

Response. Protecting dignity can justify a remedy, and that remedy can be achieved without prison. Civil damages, corrections, apologies and fines all vindicate dignity. The question is whether the incremental protection gained by imprisonment outweighs the documented abuse of custodial speech offenses, and the historical record suggests it does not.

6.3 Some falsehoods kill

Mamak (2021) proposes a narrow crime of publicly disseminating information clearly contrary to medical knowledge, to be considered only if non-criminal measures fail, pointing to the WHO's designation of vaccine hesitancy as a major global health threat. Prahassacitta and Harkrisnowo (2024) argue that Indonesia's history and social conditions can justify criminalizing fake news that disturbs public order, within limits. Governments facing ethnic violence fueled by rumors make similar arguments.

Response. Where false speech is intended to and likely to produce imminent violence, it is incitement and stays criminal under this model. For medical misinformation, Mamak himself treats criminalization as a last resort, and the public-health literature reviewed above (Pomeranz and Schwid, 2021; Marecos and colleagues, 2023) points to correction, transparency and trusted information as more effective. "Evidently contrary to medical knowledge" is also exactly the kind of standard that becomes dangerous when the government controls what medical knowledge officially is, as the Hungarian scaremongering cases illustrate.

6.4 Fines do not deter the powerful, and fines can also chill

A wealthy propagandist or a state-funded outlet can treat fines as a cost of doing business. Conversely, large civil damages and strategic lawsuits against public participation (SLAPPs) can silence journalists as effectively as prosecution.

Response. Both points are answered by careful design of the fine. Income-scaled fines and higher organizational penalties address deterrence for well-resourced actors, and anti-SLAPP rules, damages caps

and cost protections address the risk of ruinous civil claims. Imprisonment does not solve the first problem either, because powerful actors are rarely the ones prosecuted under these laws.

6.5 Democracies with strong courts can be trusted

Pritchard (2009) found that courts protected defendants in politically motivated Wisconsin cases, and Turkey's Court of Cassation overturned the first 217/A conviction. One might conclude that the solution is good judges, not lighter penalties.

Response. Judicial correction typically arrives after arrest, detention and years of proceedings, so the speaker has already been punished by the process. Judicial independence is also among the first institutions that democratic backsliding erodes. Skinner's (2016) comparison of interwar Britain and Fascist Italy is a warning that the legal tools themselves can be the same in both kinds of system; what differs is who controls them.

7. Summary of proposed changes

Based on the analysis in Section 5.1, the table below sets out, section by section, the changes we recommend to the draft Cyber Security (Amendment) Act-2027. The first column gives the section number, the second what the draft proposes, and the third what we propose instead. The last three rows contain provisions that are not in the draft but should be added.

Section	What the proposed draft contains	Our proposed change
2(aa), 2(jj)	New definitions of “disinformation” and “rumor”; “image of the state” among the examples of harm	Make knowingly false publication, refusal to correct and actual harm all mandatory elements of the definition; remove the word “image”
2(rr), 2(ff)	Definitions of “belittling” and “bullying” include ridicule, memes and edited images	Delete the definition of “belittling”; limit bullying to repeated harassment targeting a specific person; exempt satire, parody and cartoons
8(2)	Any empowered agency, including the Ministry of Information, may block content on grounds of “apprehension,” “dignity,” defamation and belittling	Blocking requests only from law enforcement, subject to tribunal approval; remove “apprehension,” “dignity,” defamation and belittling as grounds for blocking
8(3)	Obligation to publish a list of blocked content removed	Restore the obligation; a public online register
8(4)	Requirement of tribunal approval within 3 days, and restoration of content if not given, removed; appeal to the agency	Keep the provision of the current Act; appeals to an independent tribunal
12	Chairman of the National Human Rights Commission removed from the Council; Home, Foreign, and Information and Broadcasting Ministers added	Bring back the Human Rights Commission; add independent representatives of journalists and civil society
14(2)	Council meetings once every 6 months instead of every 3	Keep the provision for a meeting once every 3 months
25A (new)	Cyber defamation: 2 years’ imprisonment or a Tk 5 lakh fine	Delete the section; civil remedy; at most fines with defenses of truth, opinion and public interest
25B (new)	Belittling and bullying: 3 years’ imprisonment, non-bailable	Remove imprisonment; protective orders and income-scaled fines
26	Religious and ethnic hate publications: sentence raised from 2 to 5 years, non-bailable; “creating anxiety” is enough	Limit to incitement under the Rabat Plan criteria; remove the word “anxiety”; safeguard clause for criticism of religion and religious figures; liability for organizers of violence; fines only below the incitement threshold; bailable
26A (new)	Rumors and disinformation: 5 years’ imprisonment or a Tk 10 lakh fine, non-bailable	Remove imprisonment; first remedy an order to publish a correction; then income-scaled fines before an independent tribunal
29(3)	Suspension or cancellation of the registration, license or operations of companies, including media outlets	Delete cancellation or suspension for speech offenses; proportionate fines
46(1), 46(2)	Offenses under Sections 25B, 26 and 26A non-bailable	25A, 25B, 26 and 26A bailable and non-cognizable; written notice instead of arrest

Section	What the proposed draft contains	Our proposed change
46A (new)	Tribunal permission before arrest only for registered media	Extend this protection to all persons, including bloggers, YouTubers and independent writers
52 (new)	Civil and criminal immunity for the Council and officials for acts done “in good faith”	Delete the section; keep liability for misuse; fines for false or harassing complainants
New section	None	Safeguard clause placing criticism, satire and academic analysis of religion, scripture and religious figures, and the expression of unbelief, outside the scope of offenses
New section	None	Prohibition of imprisonment for speech offenses such as defamation, disinformation or belittling, amendable only by a supermajority
New section	None	Annual transparency report covering every case, every block, and the identity of the complainant where a public official

Table 2. Recommended changes to the draft Cyber Security (Amendment) Act-2027. Section numbers follow the comparative statement dated November 9, 2026.

These changes rest on a single principle: no one may be arrested, detained or imprisoned over speech-related matters such as defamation, disinformation, belittling or criticism of religion. Offenses such as incitement to violence, true threats, blackmail, sexual harassment and child sexual abuse material remain criminal as before, because they are defined by an act or an imminent harm.

8. Conclusion

The record from 1275 to 2026 shows speech offenses beginning with plausible goals (protecting reputations, public order, public health, national security) and repeatedly becoming instruments for imprisoning critics. Escalation follows a consistent path: vague terms, rising penalties, punishment through arrest and detention, enforcement by allies of power, and survival of the law beyond the government that created it. Democracies have not been immune, and laws written by one party have repeatedly been used by its rivals.

The most reliable safeguard is structural. If no defamation, false-news or misinformation offense can carry imprisonment or felony status, then no future government can use such a law to jail a journalist, hold an activist without bail, or remove an opposition politician from public life, however the words “false” and “harmful” are interpreted. Societies keep real tools against harmful falsehood: corrections, civil remedies, independent fact-checking, platform transparency and income-scaled fines. They also keep the criminal law for threats, incitement and fraud. What they give up is the power to put someone in a cell for what they said, a power the historical record suggests no government should be trusted to hold.

References

Peer-reviewed articles

Abcede, D., & Robie, D. (2015). Cybercrime, criminal libel and the media: From ‘e-martial law’ to the Magna Carta in the Philippines. *Pacific Journalism Review, 21*(1), 211–229. https://doi.org/10.24135/pjr.v21i1.158

Adibe, R., Ike, C. C., & Udeogu, C. U. (2017). Press freedom and Nigeria’s Cybercrime Act of 2015: An assessment. *Africa Spectrum, 52*(2), 117–127. https://doi.org/10.1177/000203971705200206

Anansaringkarn, P., & Neo, R. (2021). How can state regulations over the online sphere continue to respect the freedom of expression? A case study of contemporary ‘fake news’ regulations in Thailand. *Information & Communications Technology Law, 30*(3), 283–303. https://doi.org/10.1080/13600834.2020.1857789

Anstey, B. J. (2017). Criminal defamation and reputation as ‘honour’: A cross-jurisdictional perspective. *Journal of Media Law, 9*(1), 132–153. https://doi.org/10.1080/17577632.2017.1311467

Aryana, A. N., Akbar, M., Farid, M., & Sonni, A. F. (2026). Legal chilling effects in the algorithmic public sphere: A communicative framework for digital expression criminalization in emerging democracies. *Frontiers in Human Dynamics, 8*, 1831523. https://doi.org/10.3389/fhumd.2026.1831523

Bhowmik, S., & Fisher, J. (2026). Defensive journalism in Bangladesh: Consequences of the Digital Security Act on journalism practice. *Digital Journalism, 14*(1), 147–166. https://doi.org/10.1080/21670811.2024.2406861

Coenen, M. (2012). Of speech and sanctions: Toward a penalty-sensitive approach to the First Amendment. *Columbia Law Review, 112*(5), 991–1054.

Hunt, T. L. (2017). Servants, masters and seditious libel in eighteenth-century England. *Book History, 20*(1), 83–110. https://doi.org/10.1353/bh.2017.0002

Jenkins, D. (2001). The Sedition Act of 1798 and the incorporation of seditious libel into First Amendment jurisprudence. *American Journal of Legal History, 45*(2), 154–213. https://doi.org/10.2307/3185366

Kanstroom, D. (2020). [Review of the book *Criminal dissent: Prosecutions under the Alien and Sedition Acts of 1798*, by W. Bird]. *Journal of Interdisciplinary History, 51*(3), 480–482. https://doi.org/10.1162/jinh_r_01607

Lacy, M., & Mookherjee, N. (2020). ‘Firing cannons to kill mosquitoes’: Controlling ‘virtual streets’ and the ‘image of the state’ in Bangladesh. *Contributions to Indian Sociology, 54*(2), 280–305. https://doi.org/10.1177/0069966720917923

Leonard, Z. (2024). Libels, licenses, liberties: Conceptualising freedom of speech in colonial and postcolonial India. *Journal of Imperial and Commonwealth History, 52*(4–5), 569–599. https://doi.org/10.1080/03086534.2024.2344244

Lilienthal, G., & Ahmad, N. (2018). Sedition: A slippery slope argument devised to protect the state’s magnates. *Commonwealth Law Bulletin, 44*(4), 588–606. https://doi.org/10.1080/03050718.2019.1673199

Lisby, G. C. (2004). No place in the law: The ignominy of criminal libel in American jurisprudence. *Communication Law and Policy, 9*(4), 433–487. https://doi.org/10.1207/s15326926clp0904_4

Mamak, K. (2021). Do we need the criminalization of medical fake news? *Medicine, Health Care and Philosophy, 24*(2), 235–245. https://doi.org/10.1007/s11019-020-09996-7

Marecos, J., Shattock, E., Bartlett, O., Goiana-da-Silva, F., Maheswaran, H., Ashrafian, H., & Darzi, A. (2023). Health misinformation and freedom of expression: Considerations for policymakers. *Health Economics, Policy and Law, 18*(2), 204–217. https://doi.org/10.1017/S1744133122000263

Mayeux, S. (2021). [Review of the book *Criminal dissent: Prosecutions under the Alien and Sedition Acts of 1798*, by W. Bird]. *Journal of the Early Republic, 41*(1), 132–135. https://doi.org/10.1353/jer.2021.0010

Mittal, A. K. (2016). Implication of Shreya Singhal judgment on sedition law. *Statute Law Review, 37*(3), 273–278. https://doi.org/10.1093/slr/hmv041

Nelson, H. L. (1959). Seditious libel in colonial America. *American Journal of Legal History, 3*(2), 160–172. https://doi.org/10.2307/844283

Page, A. (2009). The Dean of St Asaph's trial: Libel and politics in the 1780s. *Journal for Eighteenth-Century Studies, 32*(1), 21–35. https://doi.org/10.1111/j.1754-0208.2008.00108.x

Pomeranz, J. L., & Schwid, A. R. (2021). Governmental actions to address COVID-19 misinformation. *Journal of Public Health Policy, 42*(2), 201–210. https://doi.org/10.1057/s41271-020-00270-x

Prahassacitta, V., & Harkrisnowo, H. (2024). The criminalization of fake news: Critique on Indonesia's new penal code. *Criminal Law Forum, 35*(1), 83–120. https://doi.org/10.1007/s10609-024-09478-y

Pritchard, D. (2009). Rethinking criminal libel: An empirical study. *Communication Law and Policy, 14*(3), 303–339. https://doi.org/10.1080/10811680903000989

Rakove, J. N. (2022). [Review of the book *Criminal dissent: Prosecutions under the Alien and Sedition Acts of 1798*, by W. Bird]. *American Historical Review, 126*(4), 1648–1649. https://doi.org/10.1093/ahr/rhab588

Rushton, P. (2015). The rise and fall of seditious words, 1650 to 1750. *Northern History, 52*(1), 68–84. https://doi.org/10.1179/0078172X14Z.00000000078

Shelton, D. (2015). Konaté v. Burkina Faso. *American Journal of International Law, 109*(3), 630–636. https://doi.org/10.5305/amerjintelaw.109.3.0630

Sherstoboeva, E. (2024). Russian bans on 'fake news' about the war in Ukraine: Conditional truth and unconditional loyalty. *International Communication Gazette, 86*(1), 36–54. https://doi.org/10.1177/17480485231220141

Skinner, S. (2016). Crimes against the state and the intersection of fascism and democracy in the 1920s–30s: Vilification, seditious libel and the limits of legality. *Oxford Journal of Legal Studies, 36*(3), 482–504. https://doi.org/10.1093/ojls/gqv034

Sonkar, A. (2026). Sedition recast: Analysing Section 150 of the BNS in light of the right to free speech. *Social Sciences & Humanities Open, 13*, 102276. https://doi.org/10.1016/j.ssaho.2025.102276

Spaic, A., Nolasco, C., & Novovic, M. (2016). Decriminalization of defamation: The Balkans case, a temporary remedy or a long term solution? *International Journal of Law, Crime and Justice, 47*, 21–30. https://doi.org/10.1016/j.ijlcj.2016.05.002

Stone, G. R. (2004). Free speech in World War II: "When are you going to indict the seditionists?" *International Journal of Constitutional Law, 2*(2), 334–367. https://doi.org/10.1093/icon/2.2.334

Taylor, L., & Pritchard, D. (2018). The process is the punishment: Criminal libel and political speech in Canada. *Communication Law and Policy, 23*(3), 243–266. https://doi.org/10.1080/10811680.2018.1467155

Teo, M. W. R., & Kiu, Y. Y. (2021). Burden of proof and false statements of fact under the Protection from Online Falsehoods and Manipulation Act 2019. *Singapore Academy of Law Journal, 33*(1), 760–776.

Vese, D. (2022). Governing fake news: The regulation of social media and the right to freedom of expression in the era of emergency. *European Journal of Risk Regulation, 13*(3), 477–513. https://doi.org/10.1017/err.2021.48

Yadav, V. (2023). The sedition conundrum in India: A critical examination of its historical evolution, current application and constitutional validity. *International Annals of Criminology, 61*(2), 1–35. https://doi.org/10.1017/cri.2023.19

Yücel, A. (2025). Hybrid digital authoritarianism in Turkey: The 'censorship law' and AI-generated disinformation strategy. *Turkish Studies, 26*(1), 1–27. https://doi.org/10.1080/14683849.2024.2392816

Zafarullah, H., & Nughat, S. (2026). Regulatory control and self-censorship in social media: Stifling freedom of expression in Bangladesh. *Journal of Asian and African Studies, 61*(6), 4733–4746. https://doi.org/10.1177/00219096261437744

Legal instruments and court decisions

UN Human Rights Committee. (2011). *General comment No. 34: Article 19, freedoms of opinion and expression* (CCPR/C/GC/34), paras. 47 and 48.

UN Office of the High Commissioner for Human Rights. (2012). Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (A/HRC/22/17/Add.4, appendix).

Parliament of Bangladesh. (2026). Cyber Security Act, 2026 (Act No. 81 of 2026). Bangladesh Gazette, Extraordinary, April 10, 2026.

Parliament of Bangladesh. (2026). Cyber Security (Amendment) Act, 2026 (Act No. 99 of 2026). Bangladesh Gazette, Extraordinary, July 1, 2026.

Proposed amendments to the Cyber Security Act, 2026: Comparative statement of the current Act and the proposed Cyber Security (Amendment) Act-2027 (version without comments, November 9, 2026).

UN Human Rights Committee. (2011). *Adonis v. Philippines*, Communication No. 1815/2008.

African Court on Human and Peoples' Rights. (2014). *Lohe Issa Konaté v. Burkina Faso*, Application No. 004/2013.

Constitutional Court of Zimbabwe. (2014). *Madanhire and Another v. Attorney General*.

High Court of Kenya. (2017). *Jacqueline Okuta & another v. Attorney General & 2 others*, [2017] eKLR, Petition No. 397 of 2016.

Constitutional Court of Lesotho. (2018). *Peta v. Minister of Law, Constitutional Affairs and Human Rights*, CC 11/2016.

ECOWAS Community Court of Justice. (2022, March 25). *SERAP v. Federal Republic of Nigeria* (Cybercrime Act s.24).

Supreme Court of India. (2015). *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; (2022). *S.G. Vombatkere v. Union of India* (interim order, May 11, 2022).

Supreme Court of the United States. (1919). *Debs v. United States*, 249 U.S. 211.

Constitutional Court of Hungary. (2020). Decision 15/2020 (VII. 8.) AB on Section 337(2) of the Criminal Code.

Singapore. Protection from Online Falsehoods and Manipulation Act 2019, s.7.

Reports and news sources for recent events

Riaz, A. (2022). *The unending nightmare: Impacts of Bangladesh's Digital Security Act 2018*. Centre for Governance Studies. https://cgs-bd.com

International Commission of Jurists. (2013). *Bangladesh: Information and Communication Technology Act draconian assault on free expression*. https://www.icj.org

Riaz, A. (2021, December). How Bangladesh's Digital Security Act is creating a culture of fear. Carnegie Endowment for International Peace. https://carnegieendowment.org

The Daily Star; The Financial Express; bdnews24.com. (2025, May). Reporting on approval and gazetting of the Cyber Security Ordinance 2025.

Internet Freedom Foundation; Supreme Court Observer. (2021–2022). Reporting on continued registration of Section 66A cases and the Supreme Court's October 2022 order.

Reuters; AFP; ARTICLE 19. (2018). Reporting on Malaysia's Anti-Fake News Act, the first conviction and the repeal vote.

POFMA Office; Singapore Police Force. (2024–2026). Media statements on POFMA offences and the first Section 7 prosecution.

Bloomberg; Reporters Without Borders; IFJ. (2020). Reporting on Hungary's emergency scaremongering provision.

OVD-Info; Novaya Gazeta Europe; Euronews. (2022–2026). Reporting on prosecutions under Article 207.3 of the Russian Criminal Code.

bianet; International Press Institute; Committee to Protect Journalists; Stockholm Center for Freedom; European Federation of Journalists. (2023–2026). Reporting on prosecutions under Article 217/A of the Turkish Penal Code.

Dawn; Voice of America; Amnesty International. (2025). Reporting on the Prevention of Electronic Crimes (Amendment) Act 2025, Pakistan.

BenarNews; Al Jazeera; Reuters; Voice of America. (2020–2024). Reporting on the cyber-libel conviction and appeals of Maria Ressa and Reynaldo Santos Jr.

Southern Africa Litigation Centre; Columbia Global Freedom of Expression. (2017–2018). Case summaries of *Okuta* and *Peta*.

SERAP; Premium Times; Media Rights Agenda. (2022–2025). Reporting on the ECOWAS Court ruling and the Cybercrimes (Amendment) Act 2024.

National Archives; National Constitution Center; New England First Amendment Coalition. Historical summaries of the Debs prosecution and Sedition Act of 1798 prosecutions.