State Surveillance versus Digital Privacy: Evaluating the Cyber Security Act Against the ICCPR

Joy Majumder[1]

ABSTRACT

The Cyber Security Act, 2023 introduced by the Bangladesh legislature was enacted to minimize digital risks. However, the law gives sweeping powers to law enforcement. Again, without the benefit of prior judicial sanction police officers can intercept private communications; seize devices and conduct digital searches. The legislation also requires internet service providers to keep user data indefinitely.

This framework assesses the Act against the privacy standards set out in international human rights law, specifically Article 17 of the International Covenant on Civil and Political Rights (ICCPR). It assesses the law against tests of proportionality and necessity from international human rights standards, specifically ICCPR. The present framework fails to meet these international standards, since it includes scope for arbitrary state intervention without sufficient procedural safeguards.

To illustrate these legal gaps, this study compares constitutional privacy jurisprudence in India and Bangladesh. The proportionality test of state data intervention is robust and strict in Indian courts. The Bangladeshi legal framework largely lacks a dedicated and comprehensive data protection law, which exists in the form of fragmented protections through national constitutional provisions framed under Article 43.

The article proposes specific statutory amendments to protect civil liberties. Lawmakers must require strict, predefined judicial warrants for all digital searches and data interceptions. The government must establish a fully independent Data Protection Authority to audit state surveillance programs. Finally, the legislation needs mandatory data minimization and destruction protocols to prevent the permanent storage of citizen data. These changes will ensure domestic cybersecurity measures comply with international human rights obligations.

[1] Student at Gopalganj Science and Technology University, Bangladesh.

KEYWORDS

Cyber Security Act 2023, Digital Privacy, State Surveillance, ICCPR, Bangladesh Constitutional Law.

INTRODUCTION

Today's digital world gives governments unprecedented power to listen in on people's conversations, steal private information, and keep track of their moves by using electronic devices. Under the guise of national security and stopping cybercrime, governments around the world explain gaining more surveillance powers. Because of the conflict between individual freedom and group safety, there must be strict laws to stop widespread abuse. The Digital Security Act of 2018[2] was replaced by the Cyber Security Act 2023[3], which was made by the government of Bangladesh to deal with new digital threats and protect important information assets. Legal experts are still arguing about whether this new set of laws guards people's basic privacy rights sufficiently. Recently published court documents establish that under the old law, hundreds of people were jailed for online protest and dozens of news websites were blocked.[4]

LAW JURIST LEGAL JOURNAL

Does the Cyber Security Act protect digital privacy from being invaded by the government without a good reason? This article argues that the law gives police too much freedom of choice when it comes to digital search and seizure operations. It does not pass the strict tests for balance and necessity set by the International Covenant on Civil and Political Rights (ICCPR).[5] When domestic law does not have certain procedural safeguards, it breaks foreign agreements and makes it easier for unconstitutional overreach to happen.

The following sections analyze the legal language of the Cyber Security Act 2023. The study compares the local legal system to international human rights standards when it comes to interference without a reason. The piece then looks at similar cases from India and Bangladesh to show how courts interpret constitutional privacy protections against government surveillance. Lastly, the study gives clear, specific suggestions for how laws can be changed to make them more in line with international standards. Lawmakers can protect web

[2] Digital Security Act, 2018, No. 46, Acts of Parliament, 2018 (Bangl.).
[3] Cyber Security Act, 2023, No. 17, Acts of Parliament, 2023 (Bangl.).
[4] Abdul Aziz, *Digital Pitfalls: The Politics of Digitalization in Bangladesh*, 14 COMMUNICATION, CULTURE & CRITIQUE 529 (2021).
[5] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

infrastructure and basic civil rights at the same time by requiring strict warrants and setting up independent oversight mechanisms.

THE DOMESTIC LEGAL FRAMEWORK

The Cyber Security Act 2023 is Bangladesh's main digital offense and data regulation law. Police have broad authority to investigate cybercrimes under the legislation. The Act allows authorities to inspect property, confiscate digital devices, and intercept conversations.[6] These broad powers frequently require little court approval. Researchers say cybersecurity legislation, while reducing cyber dangers and protecting online infrastructure, often allow governments to dominate digital environments at the expense of individual liberties.[7] Data shows that law enforcement and governing party affiliates started most of these proceedings to suppress critical news using broad statutory language.[8] Ambiguous language in the law allows authorities to expand their investigation capabilities. This imprecision shifts attention from public safety to government consolidation.

Bangladeshi law guarantees private rights. Article 43 ensures the right to home security against unauthorized access, search, and seizure.[9] The article safeguards correspondence and communications privacy. Despite these constitutional safeguards, privacy laws are scattered, creating an inconsistent regulatory environment.[10] The Cyber Security Act fits this fragmented system. Police have unlimited access to a massive pool of highly personal information when they take a computer or mobile device without a warrant. The Act does not define reasonable suspicion for such intrusive procedures.

Additionally, domestic law struggles to apply international human rights rules directly. The Supreme Court of Bangladesh has held that universal human rights rules are not directly enforceable until the legislature specifically adopts them into domestic legislation.[11] This dualist approach means citizens cannot challenge governmental monitoring in local courts

[6] Cyber Security Act, 2023, § 43, No. 17, Acts of Parliament, 2023 (Bangl.).
[7] Shamsad Binte Ehsan & Md Najmus Saquib, *Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023*, 8 J. CREATIVE WRITING 85 (2024).
[8] CENTRE FOR GOVERNANCE STUDIES, THE DIGITAL SECURITY ACT, 2018 AND ITS IMPLICATIONS FOR HUMAN RIGHTS (2022).).
[9] BANGLADESH CONST. art. 43.
[10] MT Islam et al., *Understanding GDPR: Its Legal Implications and Relevance to South Asian Privacy Regimes*, 13 UUM J. LEGAL STUD. 45 (2022).
[11] LM Kawser Ahmed, *Judicial Activism in Bangladesh: A Golden Mean Approach*, 11 INT'L J. CONST. L. 547 (2013).

using international treaties alone. Domestic laws and constitutional provisions must provide remedies. The Cyber Security Act grants government officers blanket protections for good faith activities, limiting these remedies. This broad protection prevents digital privacy violations victims from suing authorities.

By law, Internet service companies have to answer questions and keep user data for as long as they are asked. This rule on data keeping makes sure that people are always being watched. People who use the internet must leave a digital trail that the government can access. The law does not say how long data can be kept or how it can be deleted after an illegal investigation. Without these procedural protections, the right to privacy is violated, and law enforcement rights are given more weight than civil liberties.

INTERNATIONAL HUMAN RIGHTS STANDARDS

The International Covenant on Civil and Political Rights sets the global privacy standard.[12] Bangladesh signed this deal, mandating it to follow it. Article 17[13] of the Covenant says that people cannot randomly or illegally get in the way of someone else's privacy, family, home, or communication. The UN Human Rights Committee has given a lot of help in figuring out how to read this Article in the context of digital surveillance. Legal experts say that Article 17 was not even thought about when the treaty was being made. On the other hand, General Comment 16 set clear, legally binding limits on meddling.[14] "Unlawful" means that participation is not allowed unless it is required by written law. The law must follow the Covenant's goals. The word "arbitrary" makes security stronger. As a result, it makes sure that legal involvement is always fair and never used to bother or scare people.

International human rights law says that for state tracking to be reasonable, it must be necessary and fair. The government must show that it needs to invade someone's privacy to stop a major crime. For monitoring to be proportional, it must be the least invasive way to reach a legal goal. Mass surveillance and digital searches that do not need an order go against basic principles. They do not pick crime suspects based on facts when they collect data; they do it at random.

[12] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
[13] UN Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), UN Doc. HRI/GEN/1/Rev.1 (Apr. 8, 1988).
[14] Vivek Krishnamurthy, *A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy*, 114 AJIL UNBOUND 26 (2020).

International law says that people have the right to a fair hearing before their freedom is limited, but mass surveillance methods do not take this into account.[15]

These foreign rules are broken by the 2023 Cybersecurity Act. By letting police search based on vague accusations instead of proof that has been proven by a judge, the law allows for arbitrary interference. The UN keeps telling countries that they need to set up independent watchdogs to keep an eye on spying. Under human rights law[16], a check must be approved by a judge. Abuse by the government cannot be stopped by internal executive control or reviews done after the fact. Bangladesh's laws do not have an independent watchdog that can check digital surveillance orders for reasonableness and necessity.

COMPARATIVE JURISPRUDENCE: INDIA AND BANGLADESH

Courts in South Asia are beginning to recognize the centrality of digital privacy in modern life. However, the level of constitutional privacy protections available in various countries is significantly determined by their courts; as such, contrasting Indian and Bangladeshi jurisprudence demonstrates widely different judicial strategies and overall outcomes. The opportunity to review the judgment has arisen when India faced one of the historic judgments in *K.S. Puttaswamy v. Union of India at Supreme Court, 2017*.[17] In 2017, a nine-judge bench unanimously acknowledged that right to privacy was an integral component of the right to life and personal liberty under Article 21 of Indian Constitution. The Indian Supreme Court articulated a stringent three-part test for any state infringement on privacy. The state action must be predicated upon a valid law, pursuing a legitimate state aim and proportionate in the strict sense to that aim.

The Puttaswamy verdict expressly rejected the idea that a state with unlimited power to store, process and retain its citizen data unaffected by strong arm legal restraints. Previously, the Indian Supreme Court in *People's Union for Civil Liberties (PUCL) v. Union of India, 1997*[18], had declared arbitrary wiretapping unconstitutional and invariably subject to procedural safeguards, a threshold standard recently reiterated for digital restrictions in *Anuradha Bhasin v Union of India, 2020*.[19] In Bangladesh, the privacy protection under constitutional law is

[15] Natalie Garcia, *Establishing Control Order Regimes: The International Human Rights Law Implications for Pre-Conviction and Post-Release Control Orders*, 56 VAND. J.
[16] U.N. Human Rights Committee, *supra* note [13], ¶ [8].
[17] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[18] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[19] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

mainly focused on the interpretation of Article 43. Recognizing this, the Supreme Court of Bangladesh has construed this provision to prohibit unchecked state forays into private domains. In *Bangladesh v. HM Ershad, 1993*[20], the court laid down that no police or other officers can go into anybody's house and conduct a search unless he is specifically, lawfully empowered to do so. The State restriction must have a proximate, rational nexus to the constitutional limitations at issue state security and public order among others.

However, where the law does not spell out a procedure to control arbitrary or illegal exercise of search and seizure powers, it is rendered violative. In a similar fashion, in *Bangladesh Legal Aid and Services Trust (BLAST) v. Bangladesh*, *2003*[21], the Supreme Court curtailed police powers of arrest without warrant and laid down procedural guidelines that ought to compulsorily govern digital search and seizure as well. The application of such constitutional approach to Cyber Security Act 2023 exposes deep-rooted legal loopholes. Indian courts seek to read in proportionality requirements into all surveillance laws, whereas courts (of which two divisions of the Supreme Court are one), have traditionally stuck to strict textual interpretation of statutes. This problem is aggravated in Bangladesh because there is no holistic stand-alone data protection law.

Absence of a legislative structure that defines specifically how personal data would be processed, stored or retained by various public and private bodies, mean the significant powers afforded to an authority under the Cyber Security Act flow almost unchallenged. The constitutional right to avoid random search and seizure must be fully extended to the digital world. Both a physical house and a digital phone contain some highly sensitive personal information. The strong legal protections provided to physical spaces in Article 43 are equally applicable to digital communications and stored information on computers.

CRITICAL ANALYSIS AND PROPOSED SOLUTIONS

An examination of the Cyber Security Act 2023 demonstrates systemic imbalances in legislation favoring state security aims over privacy rights. This statute takes precedence over necessary procedural due process with speedy law enforcement action. This power imbalance will create a significant chilling effect on free expression and free communication online. Due to the threat of being unnecessarily surveilled and prosecuted by the state, citizens censor

[20] Bangladesh v. HM Ershad, (1993) 45 DLR (AD) 48.
[21] Bangladesh Legal Aid and Services Trust (BLAST) v. Bangladesh, (2003) 55 DLR 363.

themselves in their online activity or political discourse. The legislation has a significant legal flaw: it grants far reaching discretionary power to investigating police officers without the necessity of independent, prior judicial approval for data access.

The legislature should pass certain statutory changes to cure these legal deficiencies. The statute itself should first explicitly mandate that a judicial warrant is required for each digital search, device seizure and data interception. Before a judge issues an order to conduct a surveillance, law enforcement agencies must present concrete, articulable facts that indicate probable cause. The warrant must also name the specific data requested, the devices to be searched, and a non-renewable deadline for the surveillance operation. The warrant requirement may only be evaded in emergencies, and the exception must be specific as to both conduct and location in the law and present within twenty-four hours for judicial review. Second, the government needs to create a singular and empowered Data Protection Authority. This oversight board should have the legal ability to audit state surveillance programs, investigate civilian complaints and verify adherence to privacy laws.

The authority needs to be completely independent of the executive and report directly to the legislative branch. It would assess the extent to which data retention requirements placed on internet service providers satisfy the necessity and proportionality criteria established by international law. Third, the Cyber Security Act should stipulate both mandatory data minimization and destruction protocols. State agencies shall not subsequently hold on to any intercepted private data. Even if the investigated data is not relevant to a particular criminal investigation for which the warrant was obtained, upon conclusion of a criminal investigation, the state must permanently dispose of any remaining data. By creating statutory time limits on data retention, permanent non-consensual citizen profiles cannot be created, and potential future abuse of the data is minimized.

CONCLUSION

The Cyber Security Act 2023 is crucial to Bangladesh's security infrastructure. Current legislation does not protect digital privacy. Laws allow unauthorized state intrusion, giving police agents broad discretion to search digital devices and access private communications. Under the International Covenant on Civil and Political Rights, this legislative regime violates human rights.

These statutory flaws have substantial and extensive consequences. Since intrusive data collecting never ended, citizens risk state surveillance for every everyday activity. Without constraints on state digital surveillance, journalists, activists, and residents cannot safely communicate. India: Comparative jurisprudence shows that courts can (and should) demand absolute proportionality for state data intervention. The constitutional guarantees in Article 43 of the Bangladeshi Constitution provide robust protection, although its wide character and investigative provisions weaken its December 16 foundation.

Legislation is still needed to protect digital privacy and restore trust. The Cyber Security Act must be amended to require a "prior, strict and defined judicial warrant" to search or intercept someone's digital existence. An independent data protection authority will also provide permanent oversight of state monitoring programs. Narrow, structural improvements can protect crucial internet infrastructure while protecting citizens' civil liberties. In a secure digital environment, cybersecurity and constitutional and international human rights requirements are equal.

LAW JURIST
LEGAL JOURNAL