30 (1) 2022 IIUMLJ 33-74

ADEQUACY OF PRIVACY REGIME IN BANGLADESH: KEY CHALLENGES AND POTENTIAL POLICY MEASURES

Md. Toriqul Islam*

ABSTRACT

Privacy is one of the most desired human rights in this ubiquitous computing era - when a vast majority of our work is done online using personal data. Numerous actors are continually monitoring our activities, and consequently, user privacy came under tremendous threats. In response, various legal and policy measures have been adopted at national, regional, and international levels. The citizens of Bangladesh are also experiencing diverse privacy threats, and hence, they deserve to have adequate legal protections. This context requires a study to search for answers to the question - whether there are any legal protections for privacy in the existing legal regime of Bangladesh comparable with international data protection standards. This study aims to fill the gap using doctrinal legal research methodology. The findings of this study reveal that although there is no privacy or comprehensive data protection law in Bangladesh, privacy is conditionally recognised in the Constitution. There are numerous isolated privacy provisions in some other subsidiary legislation and references to privacy in several case laws as well. The results of this study will enlighten all stakeholders regarding privacy issues and facilitate them to map and design future policy strategies. This eventually contributes to establishing a safer online ecosystem in Bangladesh.

Keywords: Privacy challenges, Bangladesh, law, adequacy, policy.

* Research Fellow at Faculty of Law, University of Malaya, 50603, Kuala Lumpur, Malaysia, and Assistant Professor, Department of Law & Human Rights at Ranada Prasad Shaha University, Bangladesh, email: toriqul@siswa.um.edu.my (Corresponding Author)

[Received: 10 July 2021, Accepted: 24 February 2022, Published: 7 July 2022]

PENYELARASAN PRIVASI REGIM DI BANGLADESH: CABARAN UTAMA DAN LANGKAH POTENSI DASAR

ABSTRAK

Privasi adalah suatu hak asasi yang sangat diingini dalam era canggih ini, apabila kebanyakan kerja kita dilaksanakan melalui atas talian menggunakan data peribadi. Kebanyakan pelaksana berterusan memantau aktiviti kita, dan disebabkan itu, pengguna privasi mendapat ancaman yang luar biasa. Oleh yang demikian, pelbagai perundangan dan polisi telah dilaksanakan pada peringkat kebangsaan, serantau dan antarabangsa. Rakyat Bangladesh juga berpengalaman dengan ancaman privasi, jadimereka seharusnya mendapat perlindungan perundangan yang secukupnya. Konteks ini memerlukan kajian untuk mencari jawapan kepada beberapa persoalan, sama ada terdapat mana-mana perlindungan perundangan bagi privasi regim di Bangladesh dan penyelarasannya dengan tahap perlindungan data antarabangsa. Kajian ini akan mengisi jurang menggunakan doktrin metodologi perundangan. Tujuan kajian ini adalah untukmengenal pasti kebanyakan privasi cabaran berkaitan di Bangladesh; mengkaji sama ada terdapat perlindungan perundangan bagi privasi regim di Bangladesh; menilai perlindungan perundangan sedia ada dalam kaca mata tahap perlindungan data antarabangsa, dan akhir sekali, menawarkan beberapa Langkah polisi yang bersesuaian. Hasil pencarian menunjukkan bahawa walaupun tiada perlindungan privasi data di Bangladesh, tetapi privasi adalah syarat yang diperakui di bawah Perlembagaan. Terdapat beberapa peruntukan berkaitan di bawah perundangan subsidiari dan rujukan kepada kes privasi juga. Hasil kajian akan memberi pencerahan kepada semua pemegang taruh berkenaan isu privasi dan membantu mereka untuk mencorak strategi polisi akan dating. Hal ini akan memberi sumbangan kepada ekosistem atas talian yang lebih selamat di Bangladesh.

Kata kunci: Cabaran privasi, Bangladesh, undang-undang, penyelarasan, polisi.

1. INTRODUCTION

With the invention of personal computers and the Internet in the mid-20th century, the era of information begins.[1] As a result, people worldwide started using various online platforms for multiple purposes, especially, after the Internet was made open for general and public use in the 1990s.[2] This brings significant changes in the ways we communicate with one another. However, one of the pressing dilemmas of the digital age is the abundance of digital footprints. The secret data leakage of Julian Assange in 2010; Snowden's revelation in 2013; the Panama Papers leakage in 2016; the Paradise Papers disclosure in 2017, and Facebook Cambridge Analytica's scandal in 2018 shocked the global community and brought privacy issues into broad daylight.[3]

Undoubtedly, the digital atmosphere makes life easier, faster, and smarter. Simultaneously, this environment poses tremendous challenges to our information privacy as diverse actors always monitor or track our activities mostly without our knowledge. Thus, information privacy emerges as one of the pressing issues in contemporary world politics, policies, and businesses.[4]

To respond to diverse privacy challenges, there are several widely used policy measures, such as fostering privacy education; ensuring transparency in surveillance practices; conducting privacy impact assessments, and enacting data protection legislation. Among these policy options, states mostly emphasise enactment since the

---

1 Manuel Castells, *The Information Age: Economy, Society and Culture* (Oxford: Blackwell, 1996).

2 "The Birth of the Web," CERN, accessed July 9, 2021, https://home.cern/science/computing/birth-web.

3 Md Toriqul Islam, "Abu Bakar Munir, Siti Hajar Mohd Yasin and Ershadul Karim, Data Protection Law in Asia," *International Data Privacy Law* 8, no. 4 (2018): 338-40.

4 Md Toriqul Islam and Mohammad Ershadul Karim, "A Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia," *SEJARAH: Journal of the Department of History* 28, no. 2 (2019): 169.

1970s. This has been evidenced by the adoption of *Hessisches Datenschutzgesetz* (Hessian Data Protection Act) by Germany in 1970 and subsequent worldwide legal development.[5]

Meanwhile, a total of 145 countries have passed data privacy laws worldwide, while others are attempting to amend their existing legal frameworks.[6] In Asia, countries such as China, Japan, Malaysia, Singapore, South Korea, Philippines, Thailand, Bhutan and Nepal have already passed specialised data protection legislation, while India, Pakistan, and Sri Lanka are attempting to do the same. To cope with this global trend, respect citizens' right to privacy, and ensure a safer online ecosystem, Bangladesh should also establish an adequate data privacy regime.

Against this backdrop, this article aims to identify major privacy challenges in Bangladesh; explore legal protections for privacy; evaluate the adequacy of the current privacy regime considering the international data protection standards, and offer certain specific policy options.

It is worth mentioning here that there is no consensus in the literature regarding the underlying meaning of privacy. Being a sweeping concept, it varies in diverse ways. Several authors have attempted to define privacy from different angles, but probably the simplest and most discussed one is – "the right to be let alone".[7] In the

---

5 Hessisches Datenschutzgesetz [HDSG] [Hessian Data Protection Act], Hess GVB1. I 625 (1970); Spiros Simitis, "Privacy—an Endless Debate?" *California Law Review* 98, no. no. 6 (2010): 1989-2005.; Michael D Kirby, "Transborder Data Flows and the Basic Rules of Data Privacy," *Stanford Journal of International Law* 16 (1980): 27.

6 Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance," *Privacy Laws & Business International Report* 169 (2021): 1-5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348.

7 See Thomas M. Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (2nd edition, Chicago: Callaghan & Co. 1888), 29. Famous author DeCew pointed out that the notion of 'the right to be let alone' was first articulated by Thomas Cooley in his Treatise on the Law of Torts (1880), approximately a decade before the publication of the famous article by Warren and Brandeis. DeCew also noted that the term 'privacy' was evoked for the first time in a court decision in 1881 in *DeMay v Roberts*, 9 N.W. 146, 46 Mich. 160 (1881). See Wagner DeCew

information age, this typical definition cannot ensure the minimum protection of privacy if that is not associated with control over information. Hence, many scholars, including Westin, Moore, Allen and Gavison attempted to define privacy by referring to control over information.[8] However, the modern construction of privacy includes, among others, the following: (1) the right to be let alone; (2) control over personal data; (3) intimacy, (4) personhood; (5) restricted access, and (6) secrecy.[9]

It is pertinent to mention that the phrase 'data protection' has a close affinity with privacy, though in many cases, they overlap with each other, and sometimes refer to the same thing, but are not identical. Some authors argue that 'the right to privacy and data protection are two distinct rights, both formally and substantially. Yet, there exist overlapping situations - whereby they apply to the same context.'[10] For example, privacy and data protection have been embedded as one of fundamental rights in the Charter of Fundamental Rights of the European Union.[11] It means, in the EU constitutional setting, the notion of 'data protection' emerges to add something new to privacy.

By analysing the historical development of data protection, it can further be assumed that policymakers worldwide probably opted to legalise the notion of 'data protection' by referring to the traditional

J, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press 1997).

8 See Alan F. Westin, *Privacy and Freedom*, Vol 7 (New York : Atheneum, 1967); Adam Moore, *Intellectual Property and Information Control* (New Brunswick, NJ: Transaction Publishing 2001, 2004); Anita Allen, *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Lanham, MD: Rowman & Littlefield, 2003), and Ruth Gavison, 'Information Control: Availability and Control' in Stanley Benn S and G. Gaus G (eds) *Public and Private in Social Life* (New York: St. Martin's Press, 1983) 113–34.

9 Daniel J. Solove, "Conceptualizing Privacy.," California Law Review 90 (2002): 1087.

10 Raphaël Gellert Serge Gutwirth, "The Legal Construction of Privacy and Data Protection," *Computer Law & Security Review* 29, no 5 (2013): 529.

11 See European Union, "*Charter of Fundamental Rights of the European Union. Official Journal of the European Union,"* C83, vol 53 (2010): art 7 and 8, accessed June 10, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

privacy conceptions.[12] Paying heed to all, the present author uses the term 'privacy' to denote privacy, data privacy, information privacy, or data protection unless specifically refers to 'privacy and data protection', the wider universal fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union. Specifically, this research refers to all aspects of privacy but focuses mostly on information privacy.

2. RESEARCH METHODOLOGY

This study is purely doctrinal legal research that employs qualitative data collection methods and was conducted mostly based on library resources and the experience of the researcher. To understand relevant issues, facts, and findings, widespread literature was analysed from both primary and secondary sources. This study also used the content analysis technique to conclude by way of the author's analysis. Finally, the outcomes of this research have been shared descriptively.

3. PRIVACY CHALLENGES IN BANGLADESH

We are passing a tough time in human history - when the constant progress in cutting-edge technology brings an illusion of ground-breaking progress, simultaneously, entails numerous challenges. In today's hyper-connected world, human society is witnessing numerous privacy challenges in almost all spheres of life. These ever-increasing privacy threats are caused mostly by the increasing commercialisation of personal data; globalisation of human interaction; government's inclination toward data processing; use of cloud computing; voluntary data sharing on social networking sites, and the regard for privacy as one of the human rights.[13] Eventually, privacy appears as one of the most precious, but vulnerable rights in the digital age.

---

[12] Spiros Simitis, "Reviewing Privacy in An Information Society," *University of Pennsylvania Law Review* 135, no. 3 (1987): 707-709.

[13] Christopher Kuner, Fred H Cate, Christopher Millard, and Dan Jerker B Svantesson, "The Extraterritoriality of Data Privacy Laws—an Explosive Issue yet to Detonate," *International Data Privacy Law* 3, no. 3 (2013): 147-48.

The aggregate effects of privacy threats emerge as a cyber-Pearl Harbour causing physical damages to losses of lives.[14] In the past, privacy was usually meant to refer to secrecy, seclusion, bodily integrity, or inviolability of the home, communication, and correspondence. The worldwide focus on privacy issues has shifted nowadays to information privacy. Although privacy is a global challenge with massive global implications, each nation experiences some sorts of unique privacy challenges. This paper analyses the following information privacy challenges in Bangladesh: (1) National Identification Card (NID Card) scheme; (2) the biometric scheme; (3) surveillance operations, and (4) anti-terrorism movements. Each of the above challenges has been explained in the following sub-sections.

3.1. NID Card Scheme

The data breach from an unsafe NID card preparation process is quite common as the instrument contains numerous crucial personal information of the data subjects, e.g., name; parents' name; date of birth; blood group and signature. In 2007, the Election Commission of Bangladesh (EC) started preparing a nationwide voter ID card, and eventually, the scheme turned into a NID card project.[15] The laminated paper-based NID card was replaced later by a biometric and microchip-embedded smart card to prevent the duplication and fraudulent use of the NID card and to ensure better security. The preparation of countrywide voter ID cards was quite costly, and hence, the policymakers wished for multiple usages of the NID card to justify its expenses.[16]

Shortly, the use of the NID card became a mandatory document to receive numerous public-private services. In particular, the NID card has turned into an essential instrument for obtaining at least twenty-two types of services, including opening a bank account; travel passport; driving license and electronic Tax Identification Number (e-

[14] Charlotte Duc-Bragues, "Data Breaches and Privacy Law: Lawyers' Challenges in Handling Personal Information," (JD Diss., Cornell Law School, 2015).

[15] "A Card that Fosters National Identity in Bangladesh," *BBC*, June 19, 2012, http://www.bbc.co.uk/news/world-asia-india-18261373.

[16] Ibid.

TIN).[17] Thus, citizens' NID cards and the embedded data thereof have become accessible to the countless public, private, autonomous, or other entities with no proper regulation. Some newspapers, for example, reported that law enforcement authorities found fraudulent connections among ordinary vendors, customer care officers, and mobile phone companies. During the period of mobile SIM registration, many of the above actors used fake or stolen NID information and fingerprints instead of authentic ones.[18] Hence, a 2017 report revealed that a total of 42.4% of respondents (73 out of 172), Bangladeshi citizens expressed grave privacy concerns about the government's probable exploitation of the NID card scheme for political gains.[19]

Mere collection of personal data does not cause any harm if that goes fair and lawful manner. However, the collection of personal data may become worrisome in the absence of explicit legal norms to regulate such collection and use of personal data.[20] Many scholars, members of civil society, rights activists, IT experts, and noted academics identified the NID card scheme as an area of grave privacy concerns in Bangladesh.[21] In such an atmosphere, the miscreants could easily access to personal data of the NID cardholders and use them to make money by endangering the lives of the individuals. The recent *Jahalam* case is a blatant example in this regard.[22]

---

17 Ibid.

18 Md Toriqul Islam and Mohammad Ershadul Karim, "Protecting Privacy in Biometric Data," *the Daily Star*, June 10, 2022, https://www.thedailystar.net/law-our-rights/rights-advocacy/protecting-privacy-biometric-data-1602577.

19 Ahmed et al., "Privacy, Security, and Surveillance, 8.

20 Kinfe Micheal Yilma, "Data Privacy Law and Practice in Ethiopia," *International Data Privacy Law* 5, no. 3 (2015): 183.

21 Afrose Jahan Chaity, "Handset Registration: Will BTRC Move Hurt Consumers' Privacy?," *Dhaka Tribune*, January 16, 2019, https://www.dhakatribune.com/bangladesh/2019/01/16/handset-registration-will-btrc-move-hurt-consumers-privacy/.

22 Jahalam is a 32-year-old innocent jute mill worker who was sentenced to imprisonment in an allegation of 26 corruption cases on 6 February 2016 for wrongfully identified as Abu Salek. Abu Salek was a data entry staff of the National Identity Card Registration Wing of the Election Commission, who fraudulently used Jahalam's image and address for receiving a loan of Tk 18.72 crore from Sonali Bank, a state-run bank, in

It is worthy of note that the preparation of a nationwide NID card is one of the popular activities among governments across the globe. A 2017 report revealed that nearly 174 countries across the globe have nationwide NID card schemes,[23] although some major countries, such as Australia, Canada, the United Kingdom, and the United States, do not have such an scheme.[24] The biometric sim registration scheme appears another major privacy concern in current Bangladesh.

3.2. Biometric Scheme

Biometric refers to an automated tool of verification of persons using their biological or behavioural traits.[25] Apart from the identification of persons, biometric technology can be used for a wide variety of purposes, such as voting systems, health care systems, security of borders and education, etc. The biometric system works by comparing two sets of data of several body parts, facial features, eyes, fingerprints, DNA, and gesture, among others. In a biometric system, one set of data is inserted and preserved into the system as a template, while the other is possessed by the visitor. During the verification process, if these two

2010. Subsequently, the then deputy director of Anti-Corruption Commission filed a case in April 2012, and consequently, Jahalam was caught in place of Abu Salek who was then in absconding in India. Later, the High Court division of the Supreme Court of Bangladesh had discovered the miscarriage of justice, and as such, ordered the jail authority to release Jahalam without any delay. Finally, the victim Jahalam got the release from the Kashimpur Central Jail, Gazipur on 4 February 2019. See, Zakir Mostafiz Milu, "Jahalam and Abu Salek, A Curious Case of Mistaken Identity," *Dhaka Tribune*, February 6, 2019, https://www.dhakatribune.com/bangladesh/nation/2019/02/06/jahalam-abu-salek-a-curious-case-of-mistaken-identity.

23 "National IDs Around the World — Interactive Map," World Privacy Forum, accessed June 30, 2021, https://www.worldprivacyforum.org/2017/07/national-ids-around-the-world/.

24 Ibid.

25 Carlisle Adams, Alexander Barg, Friedrich L Bauer, Olivier Benoit, Eli Biham, Alex Biryukov, J Black, et al. *Encyclopedia of Cryptography and Security: A Springer Live Reference*, Springer-Verlag Berlin Heidelberg, 2011: 142.

sets of data appear identical, the biometric system confirms that the holder of inserted data and the current visitor is the same person.

Since biometric data contains numerous crucial personal data with full identity information, any leakage thereof may cause irreparable data losses. Although it is difficult to show the exact figure of the countries with the nationwide biometric scheme, a recent report by *Comparitech* reveals that Bangladesh is one of the 'top 15 countries having worst biometric SIM-card registration policies'.[26] The report also shows that Bangladesh and several other countries with similar biometric policies usually take fingerprints and facial images for biometric verification, allow law-enforcement authorities access without a warrant into the biometric system, and retain personal data for unspecified periods.[27]

Generally, governments can process citizens' personal information for compelling State interests, national security, defence, public safety, prevention, investigation, and other public interest purposes.[28] Nonetheless, governments cannot retain citizens' personal data for unspecified periods. Hence, the report of *Comparitech* can be regarded as justified. Presumably, there exist tremendous privacy threats encompassing biometric data in Bangladesh due to, among others, adequate legal protections. There were allegations against the '*Teletalk*', the only State-owned mobile operator in Bangladesh that the company attempted to register many of the customers' SIMs without verifying the information of the NID card.[29]

---

[26] Paul Bischoff, "Which Governments Impose SIM-Card Registration Laws to Collect Data on their Citizens?" Comparitech, accessed July 9, 2021, https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/.

[27] Ibid.

[28] See European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," (the GDPR) *Official Journal of the European Union OJL* 119, 4.5.2016 (May 25, 2018), art 23(1).

[29] Kamrul Hasan, "How Safe Is Your Biometric Data?" *Dhaka Tribune*, November 10, 2017, accessed June 11, 2022, https://www.dhakatribune.com/bangladesh/crime/2017/11/10/safe-biometric-data

Bangladesh began a nationwide mandatory biometric SIM registration scheme on 16 December 2015 but was challenged by a writ petition on 9 March 2016. In *SM Anamul Haque v. Chairman, BTRC and others*,[30] the petitioner challenged the legitimacy of the biometric SIM registration scheme claiming that the collection of citizens' data by mobile companies through the biometric process was insecure for citizens. Later, the High Court Division issued a rule asking the government to explain why the compulsory SIM registration scheme will not be declared unlawful. On 12 April 2016, the High Court, after a full hearing issued an order allowing the biometric SIM registration scheme.[31]

A High Court Division bench comprising Justice Syed Mohammad Dastagir Husain and Justice AKM Shahidul Huq instructed all mobile operators to protect citizens' personal information very strictly which had been obtained through biometric registration. The High Court also directed the EC to retain citizens' fingerprints in a secure place by utilising a strong password. The High Court further directed all mobile operators to follow strictly the norms of the applicable laws and directives of the Bangladesh Telecommunication Regulatory Commission (BTRC) that they could be issued from time to time for the SIM registration process.[32]

Apart from the above two schemes, the Government of Bangladesh started launching the IMEI registration of mobile phones to restrain illegal mobile imports, strengthen national security, increase revenue and prevent mobile-based crimes.[33] However, the above data

30 Writ Petition No. 2984 of 2016.

31 Md Toriqul Islam and Mohammad Ershadul Karim, "Protecting Privacy in Biometric Data," *the Daily Star*, July 10, 2018, accessed June 11, 2022, https://www.thedailystar.net/law-our-rights/rights-advocacy/protecting-privacy-biometric-data-1602577.

32 Staff Reporter, "Biometric SIM registration legal," last modified April 12, 2016, *the Independent*, accessed May 18, 2022, https://m.theindependentbd.com/printversion/details/40516

33 "Govt Starts IMEI Registration of Handsets," *the Daily Star*, October 3, 2017, https://www.thedailystar.net/city/bangladesh-government-starts-imei-international-mobile-equipment-identity-number-registration-handsets-1471036; "IMEI Database Opens Today," *the Daily Star*, Tue

processing schemes inevitably push citizens to be under excessive surveillance regimes.

3.3. Surveillance Operations

In the absence of adequate legal protections, arbitrary interference in private communications and correspondence may pose tremendous privacy threats in Bangladesh. Although the existing laws of Bangladesh allow law enforcement agencies to monitor private communications subject to prior approval of some authorities, such as the Ministry of Home Affairs and competent court, the law enforcement agencies rarely obtain permission from such authorities. It is often alleged that the government conducts massive surveillance operations on political opponents, journalists, and members of civil society.[34] The human rights groups oftentimes alleged that numerous government agencies, such as the National Security Intelligence (NSI), the Directorate General of Forces Intelligence (DGFI), and police sometimes hire whistle-blowers to conduct surveillance and produce reports against critics of the government.[35]

It is noteworthy that under Section 97A of the Bangladesh Telecommunication Act 2001 (as amended in 2006), the Government (Minister or State Minister in charge of the Ministry of Home Affairs) can, in the interest of State security or public order, empower the national intelligence, security or law enforcement agencies to intercept, record or collect information of any user of telecommunication service for a specific period.[36] Getting such empowerment, the Criminal Investigation Department of Bangladesh (CID) formed an 'Interception Cell' that performs duties 24/7 all year-round. Accordingly, the member of 'Interception Cell' or similar government officials can listen to the telephone conversation of any citizen without any warrant

January 22, 2019, https://www.thedailystar.net/business/news/imei-database-opens-today-1691068.

34 "Bangladesh 2019 Human Rights Report: Country Reports on Human Rights Practices for 2019," United States Department of State, accessed June 30, 2021, https://www.state.gov/wp-content/uploads/2020/02/BANGLADESH-2019-HUMAN-RIGHTS-REPORT-1.pdf.

35 Ibid.

36 The Bangladesh Telecommunication Act 2001 (as amended in 2006) (Act No. 18), Bangladesh, s 97A.

of the court or without maintaining any formal legal procedure. Thus, the provision of the amended Telecommunication Act 2006 may lead to massive data breach incidents in Bangladesh.

Furthermore, there has been a growing trend among law enforcement authorities and security forces in Bangladesh to purchase sophisticated cell phone surveillance devices, such as the international mobile subscriber identity catcher (IMSI catcher). This tool dissembles to be as the original mobile towers by stimulating mobile phones to get connected. While such a connection is established, the 'IMSI catcher' can track and locate a person from a mass gathering, and block transmissions of all devices in a particular zone.[37] Hence, the 'IMSI catcher' can interrupt one's right to free assembly, association, or expression, and simultaneously can invade one's privacy. Moreover, the 'IMSI catcher' can be used for invading one's privacy and committing actual bodily attacks.[38] It has been reported that in 2018, the Government of Bangladesh attempted to obtain such technologies from a Swedish surveillance company. Later, the Swiss export authority stopped exporting this technology to Bangladesh due to the allegation of misleading tender notice, and probable misuse of human rights in the country.[39] In such an environment, there remains a huge tension encompassing government-sponsored surveillance operations due to the lack of adequate legal safeguards.

The situation is becoming worsening day by day in Bangladesh. Sometimes, phone calls of the individuals are being recorded without the interest of the national security, sovereignty, or public interest grounds, and leaked through diverse media. Even some television

---

37 "IMSI Catchers," Privacy International, accessed June 28, 2021, https://privacyinternational.org/explainer/2222/imsi-catchers.

38 Fabian van den Broek, Roel Verdult, and Joeri de Ruiter, "Defeating IMSI Catchers," (paper presented at the 22nd ACM SIGSAC Conference on Computer and Communications Security, NY, USA, October 12, 2015), pp. 340–351.

39 Privacy International, "Updated - Amid Crackdown in Bangladesh, Government Forces Continue Spytech Shopping Spree," last modified July 30, 2019, accessed May 18, 2022, https://privacyinternational.org/long-read/2226/updated-amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree.

channels broadcasted the leaked phone call records of opposition political leaders unashamedly.[40] Although section 26 of the Digital Security Act 2018 prescribes punishments for the collection and use of identity information without consent; disclosure of electronic records, correspondence, communication, or information is punishable under section 63 of the Information and Communication Technology Act 2006; while eavesdropping is a punishable offence under section 71 of the Telecommunication Act 2001, the provisions of those laws are not properly followed.

3.4. Anti-terrorism Movements

There are allegations that the applications of some sections of the Anti-terrorism Act 2009[41] (amended in 2013) give rise to privacy threats to some extent. Let us examine some provisions of the said enactment.

Section 21(3) of the Anti-Terrorism Act renders that if a terrorist or terror group conducts any conversation or uploads a video of the commission of any crime using social media, or other online platforms, the law enforcement agencies can bring the issue before the court in the course of the investigation. There are no objectionable contents in the said provisions. However, the problem lies in the fact that the other part of this section confers evidential value to any document produced by police conflicting with the provisions of the Evidence Act, 1872.[42]

In recent years, the Dhaka Metropolitan Police (DMP) began to collect 17 types of personal information as a course of the anti-terrorism movement, especially after the Holey Artisan Bakery militant attack back on 1 July 2016.[43] To develop a 'central database', the DMP

---

40 Asif Nazrul, "Who Leak the Personal Phone Conversations?" *the daily Prothom Alo*, May 29, 2021, https://en.prothomalo.com/opinion/op-ed/who-leak-the-personal-phone-conversations.

41 The Anti-Terrorism Act, 2009 (Act No. 16), Bangladesh.

42 Allowing evidential values of the documents that are produced by police contradicts the provisions of the existing law of evidence. See, the Evidence Act, 1872 (Act No. I), Bangladesh, ss. 25-26.

43 "Bangladesh Siege: Twenty killed at Holey Artisan Bakery in Dhaka," *BBC*, July 2, 2016, https://www.bbc.com/news/world-asia-36692613; Ishaan Tharoor, "American Is Among 20 Dead In Terrorist Attack In Bangladesh," *the Washington Post*, July 2, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/07/01/terro

generally collect the following personal information of the city dwellers: name; father's name; date of birth; marital status; resident status; present and permanent addresses; religion; occupation; work address; educational qualification; mobile phone number; email ID; national ID number; passport number; contact person; names and details of the house helps, drivers, and security guards along with their photos, etc. There is always anxiety about the misuse of such data by police, as this agency is often identified as one of the most corrupt public sectors in Bangladesh.[44]

It is worth mentioning that the Bangladesh Telecommunication Act 2001 was amended in 2006 just after the countywide terrorist bombing attack by JMB (Jamaat-ul-Mujahideen Bangladesh) in 2005.[45] By that amendment, sections 97A, 97B, and 97C were added after section 97 in the said enactment. However, section 97A empowers government agencies to record suspicious phone calls. After such empowerment, there has been a frequent phenomenon to track phone calls and leak them to scandalise a person's image, especially, since 2013.[46] In most cases, the victims were from the political opposition, as reported in numerous international and national media.[47] All of these

r-attack-in-bangladeshs-capital-should-surprise-no-one/?utm_term=.2cbb81e27d8f.

44 Staff Correspondent, "Corruption Highest in Law Enforcement," *the Daily Star*, August 31, 2018, https://www.thedailystar.net/news/city/corruption-in-bangladesh-law-enforcement-agencies-most-corrupt-tib-1626589.

45 Ali Riaz, "Who Are the Bangladeshi 'Islamist Militants'?" *Perspectives on Terrorism* 10, no. 1 (2016): 2-18.

46 Nadim Hossain, "Unethical of Government to Record Phone Calls," *Dhaka Tribune*, November 7, 2018, https://www.dhakatribune.com/bangladesh/nation/2018/11/07/dr-zafrullah-unethical-of-government-to-record-phone-calls.

47 "2016 Country Reports on Human Rights Practices – Bangladesh," U.S. Department of State, March 3, 2017, https://www.refworld.org/docid/58ec8a7113.html; "Leaked Phone Conversation: What did Mahi B Chy and Mahmudur Rahman Manna Discuss," *Dhaka Tribune*, October 14, 2018, https://www.dhakatribune.com/bangladesh/politics/2018/10/14/leaked-phone-conversation-what-did-mahi-b-chy-and-mahmudur-rahman-manna-discussed; "Manna-Khoka Telephone Conversation Leaks', *the*

appear to be the gross infringement of the right to privacy as enshrined in major international human rights instruments[48] and Article 43 of the Constitution of Bangladesh.

There is no wonder that the protection of privacy is one of the major policy concerns all over the world, and Bangladesh is not an exception. In response, numerous legal and policy measures have been adopted at international, regional, and domestic levels. An adequate level of protection is also desirable to respect citizens' right to privacy in Bangladesh. This context justifies this study, as it aims to explore and assess the provisions of the existing laws of Bangladesh having privacy and data protection implications.

4. PRIVACY IN THE CURRENT LEGAL FRAMEWORK

To date, Bangladesh does not have omnibus privacy or data protection legislation like the Privacy Act 1974 of the USA; the Privacy Act, 1988 of Australia; the Personal Data Protection Act 2010 of Malaysia; the Data Protection Act 2018 of the UK, or the EU General Data Protection Regulations 2018 (GDPR). However, this does not mean that there are

Daily Sun, February 22, 2015, https://www.daily-sun.com/post/24220/MannaKhoka-telephone-conversation-leaks; "Audio Clip of Tarique's Conversation on Quota Reform Protest Goes Viral," *bdnews24.com*, April 12, 2018, https://bdnews24.com/bangladesh/2018/04/12/audio-clip-of-tariques-conversation-on-quota-reform-protest-goes-viral.

[48] International human rights instruments, which acknowledge right to privacy include, among others, the Universal Declaration of Human Rights, 1948, art 12; the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990, art 14; Convention on the Rights of the Child, 1989, art 16; International Covenant on Civil and Political Rights, 1966, art 17. Whereas the regional conventions, which contain privacy provisions include, the African Charter on the Rights and Welfare of the Child, 1990, art 10; the American Convention on Human Rights, 1969, art 11; the African Union Principles on Freedom of Expression, 2002, art 4; the American Declaration of the Rights and Duties of Man, 1948, art 5; the Arab Charter on Human Rights, 2004, art 21; the European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, art 8, and Johannesburg Principles on National Security, Free Expression and Access to Information, 1996, principle 10, etc.

no privacy-protective provisions in the existing legal regime of Bangladesh.

An examination of the current legal regime of Bangladesh reveals that privacy is conditionally recognised in the Constitution of Bangladesh, and there are several isolated privacy provisions in numerous other existing laws of the country. Besides, in several cases, the judiciary recognises numerous aspects of privacy. Hence, the major sources of Bangladeshi laws that deal with privacy or data protection issues can be grouped into the following three sub-categories, such as (1) the Constitution, (2) Other Statutory laws, and (3) Case laws.

4.1. Privacy in the Constitution

In *Dr Shipra Chow Chowdhury and another v. Government of Bangladesh and others*, the High Court Division of Bangladesh Supreme Court observed-

> *The framers of the constitution were particularly impressed by the formulation of the basic rights enumerated in the Universal Declaration of Human Rights. As we see that most of the rights enumerated in the Declaration have found a place in some form or other in Part III and some have been placed in Part II of the Constitution.*[49]

The above view has been manifested by the provisions of Part II, and Part III of the Constitution of Bangladesh. Part II contains the 'Fundamental Principles of State Policy,' and many provisions of this Part are similar to the provisions concerning the economic, social, and cultural rights of the Universal Declaration of Human Rights (UDHR), 1948. Part III incorporates the 'Fundamental Rights,' which are mostly similar to the civil and political rights of the UDHR. The rights enumerated in Part II of the Bangladesh Constitution are not judicially enforceable, but the provisions of Part III are enforceable.[50] Privacy is enumerated in Part III of the Constitution, and thus, it is one of the

---

49 2009, 38 CLC (HCD) [9178] = 29 BLD (HCD) (209) 183.

50 The Constitution of the People's Republic of Bangladesh (P. O. No. 76 of 1972), art 8.

judicially enforceable rights in Bangladesh. Article 43, for example, states-

> *Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health- (a) to be secured in his home against entry, search and seizure; and (b) to the privacy of his correspondence and other means of communication.*

The above provisions have also made one thing clear, privacy is not an absolute right, rather a conditional right, which can be guaranteed subject to several reasonable restrictions, such as the security of the State, public order, public morality, or public health.

There are several other fundamental rights as enumerated in Part III of the Constitution, which can also be extended to cover the right to privacy. For instance, Article 31 of the Constitution recognises the right to protection of the law as one of the inalienable rights for all citizens and other persons residing for the time being in Bangladesh. Hence, no action detrimental to the right to life, liberty, body, reputation, or property of any person can be taken except in accordance with the law. Article 32 of the Constitution affirms that no person can be deprived of the right to life and personal liberty saves under the provisions of the law.

The combined reading of both the provisions of Articles 31 and 32 guarantees the absolute right to life and personal liberty, which can extend to cover the right to privacy. In this regard, the decision of a leading Indian case, e.g., *Kharak Singh v. State of Uttar Pradesh*, 1963 is worth mentioning here. In this case, the Supreme Court of India held that-

> Although the majority found that the Constitution contained no explicit guarantee of a 'right to privacy', it read the right to personal liberty expansively to include a right to dignity. It held that 'an unauthorised intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common-law right of a man -an ultimate essential of ordered liberty, if not of the very concept of civilisation.[51]

[51] AIR 1295, 1964 SCR (1) 332.

In *Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors* case,[52] the Supreme Court of India issued a landmark judgement regarding the constitutional right to privacy. A nine-judge bench unanimously held that privacy is protected as a fundamental right under Articles 14, 19 and 21 of the Constitution of India. The judgement also added that being intrinsic to the right to life; privacy is ingrained in the whole of fundamental rights enshrined in the Constitution.

Privacy refers to a value that underpins human dignity and numerous other core values and freedoms. Australian Privacy Charter, for example, states- 'privacy is such a value, which underpins human dignity and other key values, e.g., freedom of association and freedom of speech'.[53] Similarly, under the combined reading of Articles 31 and 32 of the Bangladesh Constitution, no action detrimental to the right to life, liberty, body, reputation, or property of an individual can be taken.

Together with one's right to privacy of home and correspondence, the legal regime of any jurisdiction usually recognises the right to respect for private and family life unless otherwise required by the law.[54] Whilst privacy regards the right to life and personal liberty; respects the dignity of a human person; ensures private and family life; in this broader sense, almost all fundamental rights as enumerated in Article 27-44 can be under the domain of privacy.

4.2. Privacy in other Statutory Laws

Apart from the Constitution, the major sources of subsidiary laws of Bangladesh that contain numerous isolated privacy provisions can be classified into four sub-groups, such as (a) criminal laws; (b) civil laws; (c) telecommunication laws, and (d) cybersecurity laws.

---

52 Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India Aug. 24, 2017).

53 Australian Privacy Charter Council, "The Australian Privacy Charter," (1995) PrivLawPRpr 31; (1995) 2(3) Privacy Law & Policy Reporter 44, http://www.austlii.edu.au/au/journals/PLPR/1995/31.html, accessed May 19, 2022.

54 European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 UNTS 221, art 8.

4.2.1. Criminal Laws

Among the broad head of the criminal laws, the Penal Code 1860[55] is one of the most crucial pieces of legislation in Bangladesh that contain some privacy provisions. Under this Code, if anyone does something with an intent to insult the modesty of a woman, or intrude upon her privacy, such action is deemed to be an offence. Similarly, assaults or the use of criminal force on women aiming to insult their modesty is a punishable offence under the enactment.[56] To show respect for the modesty of women and their privacy, Section 509 of the Penal Code, for instance, asserts-

> Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

Besides, several other provisions of the Code indirectly protect the privacy interests, such as the provisions of criminal breach of trust,[57] criminal trespass to the house, etc.[58] Further, there can be an offence without any criminal intimidation or threat - when the accused encroaches upon the privacy interests of an individual by the distribution, processing, or circulation of indecent acts, photos, things, books, or materials.[59]

Like the Penal Code, the Code of Criminal Procedure 1898 (Cr. P.C.)[60] contains several privacy-protective provisions. For example, while conducting an arrest under this Code, certain specific formalities are maintained to respect one's right to life, bodily integrity, and inviolability of one's home or residence. Besides, neither any person nor his or her premises can be searched without a warrant of the court

---

55 The Penal Code, 1860 (Act No. 45), Bangladesh.
56 Ibid, s 354.
57 Ibid, ss 405, 407-409.
58 Ibid, ss 441-462.
59 Ibid, s 292.
60 The Code of Criminal Procedure, 1898 (Act No. 5), Bangladesh.

other than some exceptional circumstances.[61] Although the Code allows the law enforcement agencies or other authorised persons to utilise every possible measure to arrest the accused,[62] they cannot, however, break open *zanana*, or break open the inner, or outer door, or the window of a house, not belong to by the accused.[63]

Importantly, the Code requires a special mode while searching for or arresting a woman. In this regard, the Code postulates that 'to cause a woman to be searched, the search shall be made by another woman, with strict regard to decency.'[64] The respect for women's privacy has also been explicit in some other provisions. For example, the Code lays down that if an arrestee stayed in a place that belongs to a woman (not being the person to be arrested), who does not usually appear in public as of custom, she will be notified about the searching of her place, and allowed a reasonable time, and opportunity for withdrawing herself from that place before the commencement of the actual search.[65]

To respect one's financial data privacy, the Cr. P.C. does not allow a police officer of requiring a person to produce any document or thing that is kept in the custody of a bank or that relates to or is likely to disclose the bank account of such a person, save with the prior written approval of the High Court Division of the Supreme Court, or a Session Judge.[66] Moreover, unless otherwise approved by a District Magistrate; Chief Judicial Magistrate; Chief Metropolitan Magistrate; High Court Division, or Court of Session, a police officer cannot require any postal or telegraph authority to produce any document, parcel or thing of the individuals. It is immaterial whether such documents, parcels or things are essential for conducting any investigation, inquiry, trial, or proceeding under the Code or not.[67]

4.2.2. Civil Laws

[61] Ibid, ss 47 and 51.
[62] Ibid, s 46(2)(3).
[63] Ibid, s 48.
[64] Ibid, s 52.
[65] Ibid, s 48, para two.
[66] Ibid, s 94(1)(b).
[67] Ibid, s 95.

The Code of Civil Procedure 1908 (CPC)[68] also contains some provisions having privacy protection implications. For instance, the Code allows only the lawful arrest, detention, search, or seizure against a judgment debtor. Under this Code, an authorised officer, while conducting an arrest or detention against a judgment debtor, cannot enter into a dwelling-house before sunrise and after sunset.[69] As per the provisions of the Civil Code, breaking a dwelling-house is not allowed to enter into any premises, unless the judgment-debtor is the actual occupant of that premises.[70]

While arresting the judgment debtor, who stays in a room, or place of such a woman, who usually does not appear in public as of local customs, an authorised officer shall provide with notice, liberty, and reasonable time to withdraw her from that place.[71] In several other laws, [72] a similar provision of women's privacy is granted especially, for the *'pardanashin',* or '*parda nashin* '[73] woman. It is admissible that all the above-mentioned provisions of civil laws protect the privacy interests of the individuals to some degree.

[68] The Code of Civil Procedure, 1908 (Act No. 5), Bangladesh.

[69] Ibid, ss 55(1) and 62(1).

[70] Ibid, s 55 (1), para two and three.

[71] Ibid, s 55 (1), para four.

[72] The *Birod Mimangsha (Pouro Alaka) Board Ain*, 2004 (Dispute Resolution (Municipal Area) Board Act, 2004) (Act No 12 of 2004), sec 17(2); The Family Courts Ordinance, 1985 (Ordinance No. 18 of 1985), Bangladesh, sec 11.

[73] A 'pardanashin' lady is one who observed the rules of seclusion with rigidity. Many legal systems, especially, the British Indian legal system granted special legal protections, preservations, or exemptions for this sort women protection in several areas, such as in the performance of a contract, exemptions from being photographed, appearing before the court, etc. In Satish Chandra v Kali Dasi, AIR 1922 Cal 203, it was held that the 'pardanashin' refers to a woman of such category who lives in seclusion, shut in the Zenana, having no communication except behind the parda or screen with any male persons save a few near relations. One who sits behind the screen or parda, (does not appear in public in general) enjoyed the special object of protection of all British Courts. See, William Rattigan, "The "Parda Nashin" Woman and Her Protection by British Courts of Justice," *Journal of the Society of Comparative Legislation* 3, no. 2 (1901): 252-63.

4.2.3. Telecommunication Laws

Privacy of telecommunications appears as another crucial area of human rights in the digital age - when almost everyone belongs to a mobile handset with ample telecommunication facilities. Hence, like almost all other legal systems, privacy in telecommunication services is also recognised in the legal regime of Bangladesh. Together with the privacy of home and correspondence, the Constitution of Bangladesh affirms that every citizen of Bangladesh is entitled to enjoy the right to protection of privacy of all sorts of communications.[74] Arguably, the guarantee of privacy for all sorts of communications necessarily includes telecommunication privacy as well.

The Bangladesh Telecommunications Act 2001[75] is generally considered the prime telecommunication law in Bangladesh. Among others, the duties and responsibilities of the commission formed under the Bangladesh Telecommunications Act 2001, include ensuring privacy in the telecommunication sectors.[76]

Specifically, the Telecommunications Act 2001 aims to ensure the protection of privacy by prescribing punishments for several unlawful activities, such as unlawful interruption in radio and telecommunication systems;[77] receiving, reading, or disclosure of messages of others without permission;[78] intentionally listening to a telephone conversation between two persons;[79] publishing or attempting to publish unlawfully the messages sent or received by a person to another, etc.[80] Further, the enactment considers the wilful disclosure of any secret information, even by any commissioner, counsellor, officer, agent, or anyone appointed by the commission, as professional misconduct.[81]

Generally, privileged communications, e.g., the communication between a doctor and a patient, or an advocate and a client cannot be

[74] The Constitution of Bangladesh, art 43(b).
[75] The Bangladesh Telecommunication Act, 2001.
[76] Ibid, s 30.
[77] Ibid, s 67.
[78] Ibid, s 68.
[79] Ibid, s 71.
[80] Ibid, s 83(1).
[81] Ibid, s 85.

used as evidence in the courts but have been allowed since 2006 by the amendment of the Bangladesh Telecommunications Act 2001.[82] A writ petition was filed against this provision in the Supreme Court of Bangladesh, and the Apex Court issued rules against the government asking for an explanation as to why this amended provision shall not be declared void and unconstitutional. The hearing on the writ petition is still pending, and the government did not yet reply to the rules.[83]

4.2.4. Privacy in Cybersecurity Laws

The major cybersecurity-related laws of Bangladesh, such as (a) the Information and Communication Technology Act 2006;[84] (b) the Right to Information Act 2009,[85] and (c) the Digital Security Act 2018[86] also contain some provisions concerning privacy and data protection issues.

To respect information privacy, the ICT Act 2006 prescribes diverse kinds of punishments for a wide array of unlawful activities, such as unlawful retention of electronic records;[87] access to computers and data;[88] failure to maintain books of accounts or records;[89] unauthorised access to protected systems;[90] disclosure of confidentiality and privacy, etc.[91]

Above all, the enactment aims to ensure enforcement issues as well. To make sure of enforcement issues, the ICT Act 2006 requires the setting up of one or more Cyber Tribunals to be chaired by a Session Judge, and a Cyber Appellate Tribunal, headed by a Judge of the Supreme Court. Nevertheless, the ICT law has lost its appeal considerably due to the adoption of the Digital Security Act, 2018, and

---

[82] Ibid, ss 97A, 97B and 97C.

[83] Mohammad Ershadul Karim, *Cyber Law in Bangladesh* (Wolters Kluwer, 2020), 243.

[84] The Information and Communication Technology Act, 2006 (Act No. 39), (ICT Act, 2006) Bangladesh.

[85] The Right to Information Act, 2009 (Act. No. 20), (RTI Act, 2009) Bangladesh.

[86] The Digital Security Act, 2018 (Act No. 46), (DSA, 2018) Bangladesh.

[87] ICT Act, 2006, s 9.

[88] Ibid, s 30.

[89] Ibid, s 50.

[90] Ibid, s 61.

[91] Ibid, s 63.

the deletion of some of its sections (e.g., Sections 54, 55, 56, 57, and 66) by the Digital Security Act.[92]

Although the Right to Information Act 2009 (RTI Act 2009) primarily enables citizens to receive information from specific bodies,[93] the enactment imposes some privacy obligations on diverse public sectors too.[94] Among others, the RTI ensures 'the right of access' of the data subjects, although it does not allow citizens to rectify any information about them.[95] Further, the RTI Act imposes restrictions on the disclosure of certain information, which may, if exposed, offend the privacy of the personal life of an individual,[96] and endanger the life, or physical safety of any person.[97] Furthermore, this law does not allow disclosure of any information that is given in confidence to any law enforcement agency by a person,[98] or revelation of any secret information of a person that is protected by law.[99]

Surprisingly, some authors argue that the RTI Act 2009 is such an enactment through which the data protection law could be evolved in Bangladesh. Professor Greenleaf, for example, opines that if throughout the enactment, the phrase 'data protection' is substituted in place of 'right to information'; it may turn into a fully formed data protection authority (DPA).[100] Greenleaf further remarks that this could be a possible path through which the data protection law may be evolved in Bangladesh.[101] Probably, the above claim is far from reality.

---

92 The stated sections of the ICT 2006 were deleted by section 61 of the DSA, 2018. However, the precise contents of those deleted sections were- the penalty for damage to computer, computer system, etc; punishment for tampering with computer source code; punishment for hacking with computer system; punishment for publishing fake, obscene or defaming information in electronic form, and punishment for using computer for committing an offense, respectively. See, DSA 2018, s 61.

93 RTI Act, 2009, s 4.

94 Prasad and Aravindakshan, "Playing Catch Up," 1.

95 Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford: Oxford University Press, 2014), 449.

96 RTI, 2009, s 7(h).

97 Ibid, s 7(i).

98 Ibid, s 7(j).

99 Ibid, s 7(r).

100 See, Greenleaf, Asian Data Privacy Laws, 449.

101 Ibid.

As we know that the principal goals of the RTI 2009 were, among others - to reduce corruption and ensure accountability, transparency, and good governance in all public and private spheres, not to ensure data protection.[102]

Meanwhile, the government of Bangladesh passed the Digital Security Act 2018 (DSA, 2018), which came into force on 8 October 2018 aiming to ensure digital security and safe cyberspace. While many stakeholders raised their voices on various privacy concerns in Bangladesh, the ICT adviser to the Prime Minister told in a press release that the citizens have nothing to be worried about their privacy.[103] Against this backdrop, it is essential to analyse whether the provisions of the DSA are adequate to ensure citizens' right to privacy.

On the face of it, the DSA is a digital security-related law, not a data protection legislation. For instance, the enactment was passed to ensure, *inter alia*, nationwide digital security and to make rules concerning the prevention, identification, suppression, or trial of digital crimes, and all other relevant affairs.

However, the DSA contains some provisions of punishments for numerous crimes having connections with data privacy. Showing respect to data privacy, the DSA, for instance, prescribes punishments for –unlawful access and damages to vital information infrastructures, computers, digital devices, or computer systems;[104] deliberate access to any computers, Internet networks, or databases that may affect the friendly relationship with a foreign State, goes against public order, or

---

[102] For a general discussion, see the preamble of the Right to Information Act, 2009 reads as follows- 'Whereas freedom of thought, conscience and speech is recognized in the Constitution of the People's Republic of Bangladesh as one of the fundamental rights and right to information is an inalienable part of freedom of thought, conscience and speech, and whereas……it is necessary to ensure right to information for the empowerment of the people, whereas……..it is expedient and necessary to make provisions for ensuring transparency and accountability in all public, autonomous and statutory organisations and in other private institutions constituted or run by government or foreign financing, it is hereby enacted'. See, the preamble, RTI, 2009.

[103] "Digital Security Act 2018 to Protect Citizen Data, Privacy: Joy," *Daily Sun*, October 2, 2018, https://www.daily-sun.com/post/340222/Digital-Security-Act-2018-to-protect-citizen-data-privacy:-Joy.

[104] DSA, 2018, ss 17-9, respectively.

benefit a foreign State;[105] committing or assisting to commit an offence under the Official Secrets Act, 1923 through a computer, computer network, digital network, or any other digital device;[106] unlawful assistance in the collection, or transfer of any information of a government, semi-government, autonomous, statutory body, or any financial organisation.[107] Moreover, Section 26 of the DSA 2018 prescribes punishments for the collection and usage of one's 'Identity Information' without permission.[108]

Although the phrase 'Identity Information' contains many aspects of personal data, nevertheless, it cannot be considered a conventional definition thereof. Personal data must be with regards to a natural person only,[109] not applicable to other legal entities, but are covered by the DSA, 2018. Moreover, in the said definition of 'Identity Information,' there is no reference for location data, 'IP address', 'website browsing history', or sensitive data. Thus, even though the explanation of 'Identity Information' covers some aspects of personal data, it cannot be recognised as the conventional definition of personal data.[110]

---

105 Ibid, s 27 (1)(d).

106 The Official Secrets Act, 1923 (Act No. 19), Bangladesh, s 32.

107 Ibid, s 33.

108 Under section 26, the 'Identity Information' means- Any external, biological or physical information or any other information which singly or jointly can identify a person or a system, his/her name, address, Date of birth, mother's name, father's name, signature, national identity, birth and death registration number, fingerprint, passport number, bank account number, driver's licence, E-TIN number, Electronic or digital signature, username, Credit or debit card number, voice print, retina image, an iris image, DNA profile, Security-related questions or any other identification which due to the excellence of technology is easily available. See DSA, 2018, s 26.

109 See, European Parliament and Council, "the GDPR" art 4(1).

110 I do acknowledge that the 'identity information' incorporated in section 26 of the DSA resembles personal data. What I meant to explain here is that- To be treated as a personal data, the 'identity information' shall have to be - (1) renamed as personal data like the provision of data protection law of other countries; (2) the 'identity information' shall have to be applied to the natural persons only, and it cannot cover any system that is intended by section 26, and (3) finally, location data, IP address, website browsing

Above all, the DSA, 2018 does not contain numerous other provisions that are usually covered by a conventional data privacy law. Such provisions include, among others, the rights of the data subjects; obligations of the controllers and processors; trans-border data transfer issues; data protection principles; independent supervisory authorities; effective enforcement mechanisms, etc. Hence, despite having some aspects of data privacy laws, neither the DSA, 2018 can be termed as a data protection law nor it can outweigh the utility of enacting a data protection law in Bangladesh.

4.3. Privacy in Case Laws

Striking the balance between several conflicting interests in personal freedom, property rights and privacy is often a challenge for the court as against the State power. However, in several cases, the judiciary of Bangladesh has protected diverse aspects of privacy including the privacy of home, correspondence, and communication; women's right to privacy, and financial data privacy. A brief case study on the above issues has been shared in the following.

In a partition suit, e.g., *Dr Ismat Mirza and other v. Md Mosaddek Hossain and Ors*, the petitioner claimed that if the Court allows the defendant's portion of a house to a stranger, it will infringe her privacy interests. The Court, by analysing the circumstantial evidence, observed that 'the claim of the plaintiff with regard to the infringement of privacy does not make any sense.'[111] However, such a decision was reversed in several subsequent cases.

For instance, in *Government of Bangladesh and Others v. Hussain Mohammad Ershad*,[112] it was decided that every person shall have the right to be secure in his home against any entry, search, and seizure as per Article 43 of the Constitution. Further, it was argued in several other cases that by incorporating Section 18 of the Easement Act, the legislators intended to preserve the 'privacy of the members

history, etc may be incorporated within section 26. Of course, sensitive personal data may be defined in a separate section.

111 7 BLC 90, 1893.

112 21 BLD (AD) (2001) 69.

and inmates of the undivided dwelling house'.[113] For example, 'illustration (b)' of Section 18 of the Easement Act asserts that neither the owner nor occupier of premises can open a new window therein, which could substantially intrude on his neighbour's privacy.

Likewise, the High Court Division of the Supreme Court of Bangladesh observed in *Sreemati Sobita Rani Bonik v. Sree Gouranga Prasad Acharjee and Ors* that 'the very purpose of Section 4 of the Partition Act, 1893 are – the protection and preservation of the sentiment of the co-sharers and attachment to their ancestral property, the protection of privacy of the members of the undivided family, etc.[114] Similarly, it was held in *Amena Khatun and others v. Md. Afsaruddin*, 1997 that 'the stranger purchaser, not acceptable to other members of the family, cannot reach to an undivided dwelling house and possess it forcibly'. Pertinently, Section 4 of the said enactment is worth mentioning here, which is worded as follows-

> Where a share of a dwelling-house belonging to an undivided family has been transferred to a person who is not a member of such family and such transferee sues for partition, the Court shall, if any member of the family being a shareholder shall undertake to buy the share of such transferee, make a valuation of such share in such manner as it thinks fit and direct the sale of such share to such shareholder, and may give all necessary and proper directions in that behalf.

Like privacy of home, the privacy of correspondence and communication are also recognised by some other case laws. In *Imtiazur Rahman Farooqui (Md.) (MI Farooqui) v. Bureau of Anti-Corruption and Others*, 1998,[115] a question was raised as to whether the petitioner could be bound to share, *inter alia*, the information containing the names and addresses of all clients along with the case numbers dealt by him during the period of 1-3-93 to 20-3-94. In

---

113 *Sayesta Bibi and others v. Juma Sha and others* (1989) 18 CLC (AD) [1973]/ 42 DLR (AD) (1990) 53; *Noorjahan Akhter v. A Motaleb and Ors.* (2000) 29 CLC (HCD) [3757]/ 53 DLR (2001) 256; *Hazi Shamul Alam v. Dr. Ashim Sarkar and others* (2006) 35 CLC (HCD) [8027]/ 13 MLR (HCD) (2008) 199.

114 17 BLT (HCD) 470

115 51 DLR 421.

response, Justice Mainur Reza Chowdhury observed that seeking information in this manner was an errant nature; a targeted fishing activity toward one's information; harassment to the petitioner, and accordingly, illegal.

Recently, the High Court Division of Bangladesh Supreme Court has asserted that collecting call lists or telephone conversations from public-private mobile operators without formal consent and knowledge of the persons concerned must be stopped. In the words of the court- 'it is our common experience that nowadays private communications among citizens, including their audios/videos, are often leaked, and published in social media for different purposes, and all these activities must be stopped'.[116]

Women's right to equality, freedom or empowerment may become sometimes meaningless unless backed by their privacy interests. If equality and freedom are such rights that must be entitled by every person, privacy is one of the crucial enablers by which people can access those rights.[117] Hence, together with other rights, women's privacy interest is also acknowledged in major legal systems of the world, including Bangladesh.

Among others, the forceful imposition of dress codes, particularly for women may be regarded as degrading treatment, and outrageous to women's right to privacy. In *Advocate Md. Salahuddin Dolon v. Government of Bangladesh and Others*, 2010[118] the High Court Division of Bangladesh Supreme Court, for instance, observed that the arbitrary imposition of a gender-based dress code outrages the right to privacy, especially, for women's rights, and freedom of expression as protected under the international law. Being an active member of the ICCPR, Bangladesh cannot disregard the provisions of Article 17 thereof. Article 17 of the ICCPR prohibits, among others,

---

116 *State vs Oli* (Death Reference no 61 of 2011 & Criminal Appeal no 6592 of 2011. See also "Country Reports on Human Rights Practices for 2020," United States Department of State, Bureau of Democracy, Human Rights and Labor, accessed June 28, 2021, https://www.state.gov/wp-content/uploads/2021/03/BANGLADESH-2020-HUMAN-RIGHTS-REPORT.pdf

117 Priyanshi Vakharia, "Unveiling Privacy for Women in India," *Law Review Government Law College* 10 (2019): 37.

118 39 CLC (HCD).

arbitrary or unlawful interference with one's privacy, family, home, correspondence, honour, and reputation.

Furthermore, in *Bangladesh National Women Lawyers Association (BNWLA) v. Bangladesh and others*, 2009[119] (a petition against the 'eve-teasing'), the High Court Division of Bangladesh Supreme Court emphasised several legal and constitutional rights of women,[120] including women's privacy, modesty, and secrecy as guaranteed by Section 509 of the Penal Code 1860. In several other cases, rape has been regarded as an intrusion against women's privacy right as well.

For example, in *State v. Mostafizur Rahman and another*, 2013,[121] Justice Imman Ali observed that by definition, rape is manifestly a violation of the right to privacy of women. In another case, e.g., *State v. Secretary, Ministry of Law, Justice and Parliamentary Affairs and others*, 2009,[122] Justice Imman Ali, while commenting on a child rape victim, further remarked that the Parliament should enact a robust law to - save the children from this persecution; support the victim and witness; ensure severe punishments for the criminals, and maintain privacy, confidentiality, and dignity of women.

Financial data is often regarded as one of the most important personal data, and hence, it requires strict legal protections. Accordingly, there should have specific legal protections to ensure the secrecy and security of financial data. However, in the absence of omnibus data protection legislation, it is practically impossible to ensure financial data privacy in Bangladesh. Nonetheless, there are several case laws in Bangladesh concerning the protection of financial

---

119 14 BLC (2009) 694. Case No: Writ Petition No. 5916 of 2008.

120 In the stated case, the High Court emphasised on several constitutional rights, such as the freedom of movement as guaranteed in article 36; participation of women in all spheres of national life as rendered by article 19 (3); discrimination on the ground of sex, religion etc., as ensured by article 28; guarantees of equal protection of law and to be treated in accordance with law only, as provided with article 31, and right to life and personal liberty, as ensured by article 32 of the Constitution of Bangladesh.

121 2013, 42 CLC (AD).

122 38 CLC (HCD) [5300] = 30 BLD (HCD) (2010) 369; 15 MLR (HCD) (2010) 59.

data. However, the decisions of Bangladeshi courts regarding financial data privacy are not generally unified, rather conflicting.

For example, in *Badiul Alam Majumdar v. Information Commission, Bangladesh,* 2015,[123] the petitioners asked to receive the financial statements of the political parties but were denied by the information commission. The information office referred to financial statements as confidential information of the third parties, and accordingly, they denied providing such information. However, a reversed decision was made in *Tarique Rahman v. Director-General, Bureau of Anti-Corruption,* 1999 case. In this case, the High Court division of the Supreme Court of Bangladesh observed that-

> There is no fundamental right to privacy or secrecy in respect of property and wealth of a person and therefore calling upon the petitioners to submit the statement of their properties does not violate any fundamental right guaranteed by the Constitution. The petitioners by the impugned notices have not been accused of possessing properties disproportionate to their known sources of income. Therefore, they cannot be said to interfere with the fundamental right guaranteed by Article 35(4) of the Constitution.

Having discussed the available legal remedies for privacy intrusion, now the question is - to what extent do the above-mentioned legal remedies protect citizens' right to privacy in Bangladesh, especially, in terms of the global data protection standards? The following sub-section will search for answers to this question. It is worthy of note that together with Convention 108 of the Council of Europe 1981, the OECD Privacy Principles, 1980 placed the first-generation international data protection standards; the Directive 95/46/EC represented the second-generation standards, whereas the GDPR appears as the third-generation international data protection standards.[124]

---

[123] 69 DLR (HCD) 100 (Writ Petition No. 798 of 2015).

[124] See, Graham Greenleaf, '*European' Data Privacy Standards Implemented in Laws Outside Europe*, 149 Privacy Laws & Business International Report (2017): 21; see also, Graham Greenleaf, "Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock," *Revista Uruguaya de Protección de Datos Personales* (Revista PDP), no. 4, (2019): 49-73.

5. ADEQUACY OF PRIVACY REGIME

Evaluating the adequacy of the privacy regime of a particular jurisdiction is not an easy task as there is no globally accepted criterion by which the desired adequacy can be tested. Nevertheless, by several tests, such as (a) definitional test, (b) contextual protection, (c) privacy principles, and (d) enforcement mechanisms, probably, the standard of a data protection regime can be evaluated.[125]

(a) Definitional Test

The definitional test poses questions to any legal regime as to whether it holds any law that can be termed as privacy or data protection law by definition. Data protection refers to 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[126] Starting from the Convention of the Council of Europe (Convention 108), and other subsequent data protection instruments, currently the GDPR emerges as the standard for data protection regimes in Europe. Hence, if the data protection law of a Member Nation of the EU complies with the GDPR, such a Member Nation can be assumed to have an adequate data protection regime.

There is neither any such standard in Asia nor any universally agreed upon consensus about the minimum standard like the EU by which the privacy protection regime of Bangladesh can be evaluated. Nonetheless, it is argued that a country is said to have an adequate privacy protection regime if it has a comprehensive privacy or data privacy law containing a set of minimum data privacy principles

---

125 To assess the standard of the data privacy laws of Asia, these four tests were offered by Professor Graham Greenleaf, which can also be applied to examine the adequacy of the privacy protection regime of Bangladesh. For details of these tests, see, Greenleaf, *Asian Data Privacy Laws*, 51-75.

126 This definition was developed by Brandeis, Warren, and Prosser, and later codified by Alan Westin in 1967. See, Alan F Westin, *Privacy and Freedom*, Vol. 7 (New York: Atheneum, 1967). See also, Fred H. Cate, "Principles of Internet Privacy," 32 *Connecticut Law Review* (2000): 877.

compatible with the minimum standard as set by OECD Guidelines in the early 1980s, along with provisions for specific modes of officially backed implementation.[127]

There is no comprehensive privacy or data protection law in Bangladesh that can satisfy the minimum standard of OECD Privacy Guidelines, 1980 or other global standards as established by subsequent documents, such as the GDPR, 2018. Hence, despite having numerous isolated privacy provisions in the existing laws, Bangladesh holds an inadequate privacy protection regime.

(b) Contextual Protection

By 'contextual protections', it is intended to learn about the protection that can be ensured by the contextual surroundings, such as the Constitution, treaty, human rights organisations, civil, criminal, and administrative laws, and self-regulation.[128] To respond to those questions, it is to note that although privacy is constitutionally recognised with certain conditions, these constitutional guarantees apply vertically to cover the public sectors only. When we talk about adequate protection through institutional means, then a sizeable portion of this right and associated issues go to State organisations requiring a more horizontal, careful, and balanced initiative than one bold and moving forward a single approach.[129]

In respect of treaty protection, it is to note that although Bangladesh has either accessed or ratified the ICCPR in which there are references to privacy provisions, the country did not yet sign the instrument. Now, the issue is - whether the provisions of the ICCPR are mandatory for Bangladesh. Court decisions provided that although the ICCPR is ratified by Bangladesh, the courts do not enforce any provision of the ICCPR unless the said provision is implanted in the

[127] See, Greenleaf, *Asian Data Privacy Laws*, 52.
[128] Ibid, 53.
[129] Alexander Balthasar, "Complete Independence of National Data Protection Supervisory Authorities-Second Try: Comments on the Judgment of the Cjeu of 16 October 2012, C-614/10 (*European Commission v. Austria*), with Due Regard to Its Previous Judgment of 9 March 2010, C-518/07 (*European Commission v. Germany*)," *Utrecht Law Review* 9 (2013): 26.

domestic laws.[130] Likewise, the courts of Bangladesh need not follow the decisions of courts of other jurisdictions, even though the precedents of other jurisdictions are frequently referred to and valued by Bangladeshi courts as persuasive authority in deciding cases of similar matters.[131]

In the questions of the protections of the civil, criminal, and administrative laws, it is to be noted that privacy interests are generally protected by the application of those laws, although in several cases, privacy has not been recognised in civil suits.[132] For self-regulation, it is to state that there are no provisions regarding self-regulation in major sources of Bangladeshi laws that contain privacy provisions. Moreover, there are no significant activities of any human rights organisation in Bangladesh concerning privacy issues. Based on these findings, it can be concluded that the Bangladeshi privacy regime does not meet entirely the contextual surrounding requirements as well.

(c) Privacy Principles

To evaluate the standard of a privacy regime, the third test is - whether the provisions of any legal regime satisfy at least the minimum standard of data privacy through the inclusion of core privacy principles as

---

130 See, *Dr Shipra Chow Chowdhury and another v. Government of Bangladesh and others*, 2009, 38 CLC (HCD) [9178] = 29 BLD (HCD) (209) 183; *Bangladesh National Women Lawyers Association v. Government of Bangladesh and others* 14 BLC (2009) 703; *Bangladesh v. Metropolitan Police Commissioner* 60 DLR (2008) 660; ILDC 1410 (BD 2008); *Bangladesh and another v. Hasina and another*, 2008, 37 CLC (AD); 60 DLR (AD) (2008) 90; ILDC 1409 (BD 2008); 8 May 2008, para 86; *Hussain Mohammad Ershad v. Government of Bangladesh & others*, 21 BLD (AD) 2001, 69, and *Anika Ali v. Rezwanul Ahsan*, 2011, 40 CLC (AD) [5254] = 17 BLC (AD) (2012) 77, 17 MLR (AD) (2012) 49.

131 Dhali, Zulhuda and Ismail, Privacy Protection in Bangladesh, 570.

132 *Tarique Rahman v. Director-General, Bureau of Anti-Corruption*, 1999, 28 CLC (HCD) [4709]/ 52 DLR (2000) 518; *Chairman, RAJUK and other v. Parvin Akter*, 7 BLC (AD) 167; *Anowar Hossain (Md.) and another v. Bangladesh and others*, 2005, 34 CLC (HCD) [8918]/ 57 DLR (2005) 512, and *Dr Ismat Mirza and other v. Md Mosaddek Hossain and Ors*, 7 BLC 90, 1893.

enshrined in the OECD Privacy Guidelines, 1980, and Convention 108 of the Council of Europe, 1981.[133] If the answer is negative, it can generally be concluded that the country is lacking in maintaining an adequate data protection regime.

The OECD Privacy Guidelines, 1980 offered eight core privacy principles, such as the data quality principle; purpose specification principle; use limitation principle; openness principle; security safeguards principle; collection limitation principle; individual participation principle, and accountability principle.[134] Whereas the Convention 108 of the Council of Europe, 1981 covered all OECD principles, while adding two more, such as specific provisions for special categories of data, and principles of erasure.[135] It is explicit that no law of Bangladesh includes such privacy principles that satisfy at least the minimum data protection standards as covered by the above two international instruments.

(d) Enforcement Mechanisms

Effective enforcement mechanisms may also appear as a guide to evaluate the standard of the privacy protection regime of any jurisdiction. Although there is no universally agreed-upon consensus on the standard of enforcement mechanisms of a data protection regime, the norms, rules, and procedures of the GDPR can be a guide for evaluating the adequacy of a data protection regime. In light of the above test, we can conclude that the privacy regime of Bangladesh stands too far from establishing an adequate data protection framework. Indeed, in the absence of a specific privacy or data protection legislation in a legislative framework, searching for the standard of the enforcement mechanisms seems to be meaningless.

---

[133] See, Greenleaf, "'European' Data Privacy Standards," 21; see also, Greenleaf, "Asia's Data Privacy Dilemmas," 49-73.

[134] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)," OECD, part two, principles 7-14, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborder flowsofpersonaldata.htm

[135] "Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, ETS 108," Council of Europe, chapter II, art 6, and 8, https://rm.coe.int/1680078b37

The above literature has made it clear that the privacy protection mechanisms of Bangladesh are still in a nascent stage because of several inherent drawbacks and shortcomings. Such loopholes include, among others, the lack of comprehensive data protection legislation; the patchwork of privacy provisions; the lack of adequate provisions, and non-compliance with the global data protection standards. Against such backdrops, this paper offers some suitable policy measures in the following section.

6. SUGGESTED POLICY MEASURES

In this era of the Internet of Things (IoT), an attempt to protect privacy entails many more tools, techniques, and mechanisms other than legal ones. Nevertheless, this paper has considered only the legal and regulatory tools for regulation purposes. Particularly, this article offers the following complementary measures against privacy intrusions, such as: disseminating privacy education; regulation in surveillance; conducting privacy impacts assessment, and enacting data protection legislation.

6.1. Disseminating Privacy Education

While undertaking the initiative of protecting privacy, the challenge that every government might face is low public awareness. To raise a respectful privacy culture, basic privacy education and associated knowledge should be disseminated at various levels of national life. For that purpose, the study relating to the media and the Internet may be included in the education system as one of the core life skills, and a part of wider civic education and human development programmes.[136] Arguably, basic privacy education is essential this day not only to

[136] UNCTEAD, *Data Protection Regulations and International Data Flow: Implications for Trade and Development*, edited by Nancy Biersteker, Switzerland: United Nations, 2016, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468.

ensure safe cybersecurity but also for a man to be grown as a safe digital citizen.[137]

Privacy, data protection, or cybersecurity-related courses should be offered by major law schools. The curriculum of privacy law may be designed containing, *inter alia*, the methods in which the existing legal framework identifies privacy rights and adjusts them with other conflicting interests, such as freedom of expression; application of IoT; law and order; national security; medical data; business policies; emerging technologies, etc.[138] The course should also highlight all measures that the Constitution, law of torts, other statutes, regulations, and social values recommend for ensuring the protection of privacy.[139]

Relevant national authorities, including, the education ministry, ministry of science and information & communication and university grants commission may operate diverse privacy education programmes to create awareness. More importantly, privacy and data protection issues should be placed on the government's priority list and fostered in all spheres of national life. Regrettably, like most other laws in South Asia, the laws regarding privacy are fragmented in the region, and privacy-related issues do not exist on the high priority list of the governments.[140] For making people aware of their privacy interests, all relevant stakeholders should take appropriate responsibilities on their shoulders side by side with the governments.

6.2 Surveillance Regulation

During the era of the Revolutionary War, the prime focus of the privacy intrusions was just to become free from governmental invasions.[141] Throughout the centuries, governmental intrusion upon privacy has

---

137 Egelman, Serge, Julia Bernd, Gerald Friedland, and Dan Garcia, "The Teaching Privacy Curriculum," Conference Paper, 47th ACM Technical Symposium on Computing Science Education (2016), https://doi.org/10.1145/2839509.2844619.

138 See, "Introduction to Privacy Law and Policy," Duke Law, Course No. 331, accessed July 10, 2021, https://law.duke.edu/academics/course/331/.

139 Ibid.

140 Prasad and Aravindakshan, "Playing Catch Up," 1.

141 Daniel J. Solove, "A Brief History of Information Privacy Law, Proskauer on Privacy," *GWU Law School Public Law Research*, Paper no. 215 (2016): 1, https://ssrn.com/abstract=914271

increased significantly, especially, after the terrorist attack of September 11, 2001.[142] Today's changing global contexts mandate the governments to increase surveillance operations even causing tremendous threats to privacy. This atmosphere broadens the usage of data mining practices and post-hoc behavioural approach analysis techniques. Although excessive surveillance practices significantly affect privacy interests, contrarily, there remains huge public support for government-operated surveillance operations as well.[143]

Due to the lack of comprehensive data protection legislation in Bangladesh, the current legal provisions are obscure and scattered in nature. Moreover, the provisions of some laws render law-enforcement authorities excessive surveillance powers with no binding principles. Whereas any systematic government surveillance programme is not justified unless that is transparent and grounded on proper explanations.[144] The situation compels either to enact a new law, and establish efficient monitoring bodies thereunder, or leave privacy dilemmas unchallenged. This backdrop suggests placing the unregulated surveillance practices into a specific legal framework.

6.3 Conducting Privacy Impacts Assessment

---

142 See, David Lyon, "Globalizing Surveillance: Comparative and Sociological Perspectives," *International Sociology* 19, no. 2 (2004): 135.

143 In a survey conducted by Harris Interactive & Westin between September 19–24, 2001 among 1,012 adults American, the researchers found that there existed huge public support about the increasing investigative powers of the government. While asked regarding ten distinct proposals for increased surveillance powers of the government, above 90% of people approve three of those proposals; nearly 80%-90% approve three more, and 54%-68% of the public support the rest. See, Humphrey Taylor, "Overwhelming Public Support for Increasing Surveillance Powers in Spite of Many Concerns about Potential Abuses, Confidence that those Powers would be Used Properly," Harris Poll 49, (2001), accessed June 30, 2021, https://theharrispoll.com/wp-content/uploads/2017/12/Harris-Interactive-Poll-Research-OVERWHELMING-PUBLIC-SUPPORT-FOR-INCREASING-SURVEIL-2001-10.pdf

144 Ira S Rubinstein, Gregory T Nojeim, and Ronald D Lee, "Systematic Government Access to Personal Data: A Comparative Analysis," *International Data Privacy Law* 4, no. 2 (2014): 96-119.

Privacy impact assessment (PIA) is another crucial mechanism that a country may consider in avoiding unwanted privacy challenges. The PIA refers to a systematic process for evaluating the potential impacts on the privacy of a project, initiative, proposed system, scheme, etc.[145] The PIA generally works as an 'early warning system' for both government agencies and businesses to make better-informed decisions while avoiding privacy disasters before launching any scheme.

Sometimes, governments or businesses are to withdraw a newly developed project or product due to bitter public reaction on privacy grounds. The PIA, as a policy option, can save government entities, businesses, or other stakeholders from possible damages that might have been caused by privacy reasons. A PIA report has also the potential to save both money and reputation.[146] For the proper functioning, a PIA regime shall equip with a specific legal and institutional setup. Moreover, an independent data protection authority shall have to be formed under the data protection legislation, and all stakeholders should deal with data in compliance with the PIA requirements.

6.4 Enacting Data Protection Legislation

Paying heed to all other policy measures, Bangladesh should enact a comprehensive data privacy law. A comprehensive data protection legislation is not only crucial for protecting fundamental human rights but also for ensuring privacy interests.[147] The enactment is also essential to establish an independent body for monitoring the entire data protection regime; examining the impacts of the privacy regime and carrying out other initiatives as required for the implementation of the legal rules.[148]

---

[145] Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review* 25, no. 2 (2009): 135.

[146] See, Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook* (Wellington: 2007), 11, https://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf.

[147] Vanberg, Aysem Diker, "Informational Privacy Post GDPR–End of the Road or the Start of a Long Journey?" *The International Journal of Human Rights* 25, no. 1 (2021): 52-78.

[148] Yilma, "Data Privacy Law," 189.

While considering the enactment, the next question is about the model for future data protection legislation. This paper argues that Bangladesh may enact a GDPR-styled data protection legislation since the Regulation appears as a clarion call for a unique global data privacy gold standard.[149] The GDPR refers to the 'General Data Protection Regulation', a central data protection instrument for the European Union (EU) and the European Economic Area (EEA). The lifecycle of the GDPR began in January 2012 through a proposal of the European Commission (EC), which was approved on April 27, 2016, and finally, it came into effect on May 25, 2018. It replaced the previous Directive 95/46/EC with several intense changes in almost everything, ranging from technology to advertising, and medicine to banking.[150] The official document of the GDPR is a huge, comprehensive, and complex document containing 11 chapters; 196 recitals; 99 articles, 88 pages, and 55,000 words.

7. CONCLUSION

By utilising doctrinal legal research methodology, this paper aimed to identify selected privacy challenges in Bangladesh; explore existing legal protections; evaluate their adequacy compared to international data protection standards, and offer suitable policy measures. The findings reveal that the privacy protection regime of Bangladesh is in a nascent stage due to, among others, the lack of comprehensive data protection legislation; the patchwork of privacy rules; lack of adequate provisions, and non-compliance to international data protection standards.

Against such a background, this paper recommended four suitable policy options, and specifically, it focused on enacting comprehensive data protection legislation in line with the international data protection standard. Contemplating the GDPR as a clarion call for

---

149 Giovanni Buttarelli, "The Eu GDPR as a Clarion Call for a New Global Digital Gold Standard," *International Data Privacy Law* 6, no. 2 (2016): 77.

150 Hern A, "What Is GDPR and How will It Affect You?" The Guardian, 21 May 21, 2018, https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you, accessed May 19, 2022.

global data protection regulations, this paper argues that Bangladesh should enact a GDPR-creep omnibus data privacy legislation to ensure citizens' right to privacy, cope with global trends, and establish a safer online ecosystem in the country.