UUM JOURNAL OF LEGAL STUDIES
http://e-journal.uum.edu.my/index.php/uumjls

How to cite this article:
Islam, M. T. (2022). An assessment of privacy regime in Bangladesh: A legal analysis. *UUM Journal of Legal Studies*, *13*(2), 77-108. https://doi.org/10.32890/uumjls2022.13.2.4

AN ASSESSMENT OF PRIVACY REGIME IN BANGLADESH: A LEGAL ANALYSIS

Md. Toriqul Islam
Faculty of Law, University of Malaya, Malaysia
Department of Law and Human Rights,
Ranada Prasad Shaha University, Bangladesh

toriqul@siswa.um.edu.my

Received: 2/5/2021 Revised: 10/9/2021 Accepted: 5/10/2021 Published: 21/7/2022

ABSTRACT

Privacy is one of the most valued human rights in the information age. Due to the present digital world context, privacy appears as one of the pressing problems. In a data-driven world, a vast majority of works are going online using personal data. Personal data emerge as the new fuel to the Internet, and coin to the digital world. This digital atmosphere makes life easier, faster, and smarter, while simultaneously posing tremendous challenges to privacy. Therefore, the debate encompassing privacy evolves as one of the hot-button issues in contemporary world policies, politics, and business. In response, multiple policy measures have been adopted at national, regional, and international levels. To cope with this global trend, establish a safer online ecosystem, and secure citizens' right to privacy, Bangladesh should maintain an adequate privacy protection regime. This landscape leads the current researcher to explore and assess the

privacy protection regime of Bangladesh, as there is a lack of research in this area. There is a clear gap in the existing literature that requires to be filled in, and this research aimed to fill that gap using doctrinal legal research. The findings revealed that privacy was not adequately protected in Bangladesh due to, mainly, the lack of omnibus data privacy legislation. This article concluded by offering some workable suggestions, and especially, urged for enacting comprehensive data protection legislation in Bangladesh. Presumably, this research will enlighten all stakeholders regarding an overall picture of the privacy protection regime of Bangladesh. Moreover, this study will facilitate relevant stakeholders to map their future strategies and policy directions towards establishing an effective privacy protection regime in Bangladesh.

Keywords: Privacy, importance of privacy, Bangladeshi privacy regime, assessment, suggestions and recommendations.

INTRODUCTION

In the mid-twentieth century, the information age, digital age, computer age, or media age begins with massive implications at all spheres of human life. It is a part of a historical epoch that is circumscribed by a rapid ground-breaking shift from the traditional industry-based economy to an information technology-based economy (Castells & Blackwell, 1998). Currently, the world is experiencing radical technological transformations, which bring changes in the way humans live, work, and communicate (Syed et al., 2020). In this age, the dependence on online platforms has increased significantly, and people have begun using diverse online platforms for multiple purposes, such as education, teaching, learning, business, entertainment, and socialisation. Most people, especially, the young, enjoy the advantage of limitless access to Internet-provided facilities and services (Ayub & Yusoff, 2020). However, in this digital atmosphere, the collection, retention, use, and transfer of personal data have become rampant chiefly by government agencies and business entities.

To indicate governments' aptitude towards personal data, George Orwell (2009) once warned people in his dystopian novel '*Nineteen Eighty-Four*' that 'Big Brother (a fictional character to refer to the

government authorities) is always watching you' (Orwell, 2009). The trend of government-sponsored data processing has increased over time and especially, after 9/11, 2001. This trend of data processing has tremendous implications for the contemporary privacy protection paradigm. Westin (2003), for example, remarked that the privacy landscape has changed after the incident of terrorist attacks on 11 September 2001 (Westin, 2003). Whereas business' data processing activities have also become evident by new business models, which are mostly grounded on personal data. In recent decades, privacy, especially, information privacy appears as one of the pressing concerns in the global political agenda (Islam, 2018). In such an atmosphere, ordinary citizens, being private individuals, or consumers desire to have adequate protections. Consequently, the worldwide debate on privacy concerns has become apparent, and Bangladesh is not an exception.

This context requires to have extensive research to explore and assess the data protection regime of Bangladesh but is non-existent. Therefore, there remains a clear gap in the existing literature that needs to be filled in, and the current research aims to fill that gap by offering a brief overview of the privacy regime in Bangladesh. By explaining the importance of privacy in Section 3, the Bangladeshi privacy regime in Section 4, assessing the privacy regime in Section 5, and adding some workable suggestions in Section 6, this article presents an overview of the privacy protection regime of Bangladesh.

OBJECTIVES AND METHODOLOGY

The objectives of this paper are threefold. Firstly, this paper explores the sources of Bangladeshi laws having privacy and data protection implications. Secondly, this paper evaluates whether the protection of privacy as ensured in the legal regime of Bangladesh is adequate in comparison with global data protection standards. Finally, this paper offers certain specific suggestions for the protection of privacy and personal data in the legal regime of Bangladesh.

This study adopted doctrinal, or desk-based, or library-based research methodology to achieve the desired research objectives by answering certain specific research questions. It utilised a qualitative approach

and was conducted based on library resources and the experiences of the researcher. To understand the relevant issues, facts, and findings, extensive literature was analysed from both primary and secondary sources. The findings have been shared in a descriptive manner.

IMPORTANCE OF PRIVACY

Nowadays, while cyberspace is extensively used in facilitating one to have an online profile, it also entails diverse legal issues (Mirshekari et al., 2020). In the data-based world, numerous actors continuously monitor or track people's activities, and eventually, their privacy becomes vulnerable (Islam & Karim, 2019a). The atmosphere is rightly described as 'cell phones that pinpoint your location; cameras that track your every move, and subway cards that remember. Thus, we routinely sacrifice privacy for convenience and security. So, stop worrying, and get ready for your close-up' (Penenberg, 2001). In such an environment, privacy is indispensable, and accordingly, 'one cannot violate it unless there remains a compelling State interest' (Elison & NettikSimmons, 1987). Therefore, from the cradle to the grave, privacy requires to be duly respected.

Privacy is important not only for human beings but also for other animals. The basic outcomes of animal studies revealed that every animal seeks privacy in a small-group intimacy (Westin, 1967). Westin (1967) further added, the ecological studies showed that the dearth of personal space, due to congestion and the like, may generate huge challenges to survival (Westin, 1967). Moore (2003) noticed that in case of scarcity of privacy, the beasts generally attempt to demolish them, or massively engage in the fatal decreases of their species (Moore, 2003). While experimenting rats at slots in cages, Calhoun (1950) noticed that a certain amount of free space is essential for each breed of the animals and any shortage thereof may lead to break up in an amicable relationship and cause numerous diseases, such as increased blood pressure, heart failure, etc. (Calhoun, 1950). Since human beings are likely to evolve from other species than humans, Homo sapiens likely carry the same traits.

Some scholars show that privacy is very important for democracy too, although the relationship between them is a complex and dynamic one, and there are disagreements between them in terms of meaning, dimensions, and types (Bennett & Marfo, 2019). In the recent past,

very little is understood as to how privacy is compromised in a democracy by the polling agents, who endeavour to mobilise, involve, and stimulate voters to vote, or not to vote. Lately, this manipulation of voters' psychology in social media by polling agents and its influence on the result of the election has turned to be an issue of a huge debate in the global political discourse. There are allegations against the former US President Donald Trump that his election campaigns used the voter suppression strategy in the 2016 US election by sending negative messages (dark posts) based on race, ethnicity, and socio-economic status, and using the advertising tools of Facebook (Bennett & Marfo, 2019). Therefore, the issue is no longer restricted to the privacy of the individual voter only, but rather correlates to greater trends of democratic politics as well.

Apart from a legal right, privacy can be claimed as a reasonable expectation of human beings. For this reason, people generally share any confidential matter with a minimum number of trusted persons only having a belief that these trusted people will not share the matter with any third party. Above all, in today's networked world, privacy is one of the most valued rights, as sometimes people become bound to share their sensitive personal data with numerous agencies in exchange for receiving multiple services, even knowing the vulnerability of their privacy. Consequently, it will be a disaster, if any of those bodies expose unlawfully any of people's valuable personal information. These losses will be unthinkable, as most of them are irreparable and admit no substitutes or compensations. Therefore, together with all legal theories, moral philosophy, and public policy, most theorists in the civilised world recognise the protection of the right to privacy.

The above discussion clearly demonstrates the importance of privacy for each of the species, including human beings. Each human society must have an adequate privacy protection regime within the national legal framework. This situation raises a vital question – whether Bangladesh maintains an effective privacy protection regime at the national level. The combined reading of Sections 4 and 5 of the current research will present the answer to this crucial question.

PRIVACY REGIME IN BANGLADESH

There is no comprehensive privacy or data protection legislation in Bangladesh like the Privacy Act 1974 of the USA, the Privacy Act

1988 of Australia, the Personal Data Protection Act 2010 of Malaysia, or the European Union General Data Protection Regulation (EU GDPR) 2018. This, however, does not mean that privacy protection mechanisms are completely missing in the legal regime of Bangladesh. An examination of the present legal regime of Bangladesh exhibits that privacy is conditionally recognised in the Constitution of Bangladesh, and there are several isolated privacy provisions in numerous other existing laws. Besides, in many cases, the judiciary recognises diverse aspects of privacy. The major sources of Bangladeshi laws having privacy protection implications can be classified into three categories, such as (1) the Constitution, (2) Subsidiary laws, and (3) Case laws.

Constitution

The framers of the Constitution of Bangladesh (1972) were significantly influenced by the provisions of the key international human rights instruments, particularly, the Universal Declaration of Human Rights (UDHR, 1948), and the International Covenant on Civil and Political Rights (ICCPR, 1966). This has been evidenced by the statement of the preamble, subsequent provisions as enumerated in Part II and Part III of the Constitution, and the case laws. In *Dr Shipra Chowdhury and another v Government of Bangladesh and others* (2009), the High Court Division of Bangladesh Supreme Court, for instance, observed that:

> … 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.

Privacy, in particular, the privacy of home, correspondence, communication, honour, and reputation, is recognised in major international instruments. Nevertheless, the basic foundation of privacy has been laid down by Article 12 of the UDHR, and Article 17 of the ICCPR. Being influenced by these two instruments, a similar recognition of privacy, especially, the privacy of home, correspondence, and communication, is recognised in Article 43 of

the Constitution of Bangladesh. Article 43 of the Constitution of Bangladesh is worded as follows:

> 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.

From the above provisions, it is apparent that privacy is constitutionally recognised in Bangladesh, as provided with subject to any reasonable restrictions imposed by the law. In principle, the Constitution deals with public rights only, and thus, privacy concerns in private sectors remain outside the ambit of this constitutional mandate. It is worthy of note that there are numerous aspects of privacy, and a very few of them, e.g., the privacy of the person, privacy of home, and privacy of communication, are only covered by the Constitution. Specifically, there are at least five more types of privacy outside this constitutional mandate,[1] yet they remain outside the scope of the Constitution.

It is worth mentioning that in an adequate privacy or data protection regime, there may be explicit constitutional recognition of privacy or some provisions that indirectly recognise privacy that are often established by the interpretation of courts. One source confirms that globally, the Constitutions of more than 130 countries recognise the right to privacy (Privacy International, 2017), while another source ensures that the number is over 150 national Constitutions (Constitute, 2021). Interestingly, there are many established democracies in the world, for instance, the USA and Malaysia, which maintain adequate data protection laws, but there is no explicit recognition of privacy in their Federal Constitutions. Nevertheless, in numerous cases, the judiciary of both the countries held that the provisions of privacy are generally imbedded in numerous provisions, such as the provisions of the right to life, personal liberty, etc.

[1] In a wider sense, the typology of privacy can be summarised as – bodily privacy; spatial privacy; communicational privacy; proprietary privacy; intellectual privacy; decisional privacy; associational privacy; behavioural privacy; and informational privacy. See generally, Koops, B. J., Newell, B., Timan, T., Skorvánek, I., Chokrevski, T., and Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 484.

For example, in *Sivarasa Rasiah v Badan Peguam Malaysia & Anor case* (2010), the Federal Court of Malaysia observed in the form of obiter dicta that the provisions of the right to life and personal liberty, as recognised in Article 5(1) of the Federal Constitution, include many rights, especially, the right to privacy (Islam et al., 2021). Generally, the constitutional recognition of privacy, be it explicit, or implied, covers only a minimum aspect of privacy, such as privacy of home, correspondence, communication, or bodily integrity, not all aspects thereof. A mere constitutional recognition of privacy is not enough to ensure an adequate privacy protection regime unless it is backed by omnibus privacy or data protection legislation, and together with an effective enforcement mechanism. Nevertheless, together with the constitutional protections of privacy, many subsidiary laws of Bangladesh contain provisions of some aspects of privacy, which need to be analysed for the purpose of this article.

Subsidiary Laws

Apart from the Constitution, a handful of Bangladeshi laws contain diverse isolated privacy provisions. These laws can be classified into four distinct groups, such as (a) criminal laws, (b) civil laws, (c) telecommunication laws, and (d) cybersecurity laws.

Criminal Laws

Among the criminal laws, chiefly, the Penal Code (1860) and the Code of Criminal Procedure (1898) contain some provisions having privacy protection implications. In the first phase of this sub-section, the current paper will explain the relevant privacy provisions of the Penal Code, and in the last phase, it will analyse the relevant provisions of the Criminal Procedure Code. Like many other countries, the Penal Code is one of the most important pieces of legislation in Bangladesh that contains some privacy provisions. Under this Code, if anyone does something with an intent to insult the modesty of a woman, or intrudes upon her privacy, such action is deemed to be an offence. Section 509 of the Penal Code, for example, states:

> 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.

Similarly, the assaults or use of criminal force on women aiming to insult their modesty is a punishable offence under this enactment (Penal Code. s. 354). Besides, several provisions of this Code indirectly protect privacy. For example, if a person, entrusted to any property being a carrier, clerk, servant, banker, merchant, or agent, misappropriates, converts, uses, or by any means disposes of the property to others dishonestly, unlawfully, or violating any express term of an agreement, he or she commits a crime (Penal Code. ss. 405, 407-9).

The Penal Code also respects the inviolability of one's home by incorporating provisions against criminal trespass to the house (Penal Code. ss 441-62). Unless accomplished for bona fide or religious purposes, and even without having any criminal intimidation or threat, there can be an offence, when the accused encroaches upon the privacy interests of an individual by the distribution, processing, or circulation of indecent activities, photos, things, books, or materials (Penal Code. s. 292). Furthermore, if anyone, without having any lawful authority gains any property of others, he or she commits a crime of 'wrongful gains' (Penal Code. s 23). Analogically, it can be argued that an unlawful collection, processing, or retention of personal data may be deemed as 'wrongful gains', even though it is still debatable whether personal data is a property in law or not.

Apart from the Penal Code, the Criminal Procedure Code (1898) (Cr. P.C.) contains several privacy-protective provisions as well. The Criminal Code renders certain specific formalities for conducting an arrest, search, and seizure, and eventually, respects one's right to life, bodily integrity, and inviolability of home or residence. Under this Code, neither any person nor his or her premises can be searched without a court warrant other than the exceptional circumstances (Cr. P.C. ss. 47 and 51). Although the Code allows police officers or other authorised persons to utilise every possible measure to arrest the accused (Cr. P.C. s. 46(2)(3)), such officers cannot break open the *zenana*, break open the inner, or outer door, or the window of a house

not belonging to the accused (Cr. P.C. s. 48).
Besides, the Cr. P.C. requires a special mode while arresting or searching for a woman. The enactment postulates that 'to cause a woman to be searched, the search shall be made by another woman, with strict regard to decency' (Cr. P.C. s. 52). Respect for women's privacy has also been explicit in some other provisions too. For example, the Cr. P.C. 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 the public as of custom, the police officer will notify her and let her a reasonable time and opportunity for withdrawing herself from the place, before the actual commencement of any search (Cr. P.C. s. 48, para two).

As per the provisions of the Code, the police officers or courts may require anything or any document to be produced before them, which are essential for conducting any investigation, inquiry, or trial, but such provision does not apply to financial data. Particularly, without the prior written approval of a Session Judge, or the High Court Division of the Supreme Court, an officer in charge of police cannot require anybody to produce any document or thing which is kept in the custody of a bank, or banker that relates, or likely to disclose the bank account of any person (Cr. P.C. s. 94(1)(b)). Therefore, the Code respects one's financial data by incorporating special provisions to deal with the relevant issues.

Above all, unless otherwise approved by some higher authorities, such as the District Magistrate, Chief Judicial Magistrate, Chief Metropolitan Magistrate, High Court Division, or Court of Session, the Cr. P.C. does not allow a police officer to require any postal or telegraph authority to produce any document, parcel, or thing before him, no matter how essential they are for conducting any investigation, inquiry, trial or proceeding under this Code (Cr. P.C. s. 95). As per the criminal laws, the law enforcing authorities can lawfully conduct any search, seizure, and arrest of any person (Cr. P.C. s. 46-67, 53, 523, 550); however, this Code does not allow them to require one's parcel, personal communication, and correspondence, and bring them into public. In this manner, the Code shows some sort of respect to private communications, as guaranteed also in Article 43 of the Constitution of Bangladesh.

It is noteworthy that the constitutional protections for communicational

privacy have also been reaffirmed in the *State and Ors v Oli and Ors* (2019) case. In this case, the Supreme Court of Bangladesh held that obtaining phone call records of an individual from any public-private mobile operators without formal legal requirements, such as search or seizure, or a formal request to the concerned operators and knowledge of the persons concerned infringed the constitutional right to privacy.

Civil Laws

Like the Penal Code and the Cr. P.C., the Code of Civil Procedure (1908) (CPC), (Act No. 5 of 1908) contains some isolated privacy provisions. For instance, the Civil Code allows only the lawful arrest, detention, search, or seizure against the judgment debtor. Under this Code, an authorised officer, while conducting an arrest or detention against a judgment debtor, cannot enter a dwelling house after sunset and before sunrise (CPC. ss. 55(1) and 62(1)). Moreover, breaking into a dwelling house to enter any premises is not allowed, unless the judgment-debtor is the actual occupant of such dwelling house (CPC. s. 55 (1), para two and three). Besides, if a room is under the actual possession of a woman, who usually does not appear in public as per the local customs, the authorised officer shall provide her with notice, liberty, and reasonable time to withdraw her from that room while arresting the judgment debtor (CPC. s. 55 (1), para four). In all these cases, there remains an explicit recognition of privacy of home, person, or bodily integrity.

Special provisions for the *'pardanashin*' or '*parda nashin'*woman'[2] is granted in some other civil laws. For instance, Section 17(2) of the *Birod Mimangsha (Pouro Alaka) Board Ain* (Dispute Resolution

[2] A '*pardanashin*' lady is one who observed the rules of seclusion with rigidity. Many legal systems, especially the British Indian legal system, grant special legal protections, preservations, or exemptions for this category of women's 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) enjoys the special object of protection of all British Courts. See Rattigan, W. (1901). The "Parda Nashin" Woman and Her Protection by British Courts of Justice. *Journal of the Society of Comparative Legislation*, *3*(2), 252–263.

(Municipal Area) Board Act) 2004 states that in case of the reluctance of personal appearance by a *paradanashin* woman, the Board may allow a representative, duly empowered by her, to appear before the Board on her behalf. Whereas the Family Courts Ordinance (1985) can allow camera trial on request of both the parties (Family Courts Ordinance. s. 11). All the abovementioned provisions of civil laws protect the privacy interests of the individuals to some degree.

This atmosphere, however, indicates that despite the lack of omnibus data protection legislation and contextual limitations on the application of constitutional provisions of privacy, the Civil Code, being a part of the subsidiary laws, protects some aspects of privacy. Especially by incorporating the above provisions, the Civil Code, like the Penal Code and Criminal Procedure Code, respects women's right to seclusion, solitude, or purdah, which is observed as a social custom from time immemorial in the Indian sub-continent.

Telecommunication Laws

The telecommunication laws of Bangladesh that contain several privacy provisions include, *inter alia*, the Telegraph Act (1885), the Wireless Telegraphy Act (1933), and the Bangladesh Telecommunications Act (2001). The provisions of the Bangladesh Telecommunications Act prevail on the provisions of these two laws. However, the duties and responsibilities of the commission, established under the Bangladesh Telecommunications Act include, among others, ensuring privacy in the telecommunication sectors (Telecommunications Act. s. 30).

The Telecommunications Act further ensures the protection of privacy apparently by prescribing punishments for unlawful intervention in radio and telecommunication sectors (Telecommunications Act. s. 67). To respect privacy, the enactment also prescribes punishments for an individual who receives, reads, or discloses the messages of others without proper authorisation (Telecommunications Act. s. 68); intentionally listens to a telephone conversation between two persons (Telecommunications Act. s. 71); or publishes or attempts to publish the messages sent or received by a person to another unlawfully (Telecommunications Act. s. 83(1)). Moreover, the enactment affirms that wilful disclosure of any secret information, even by any commissioner, counsellor, officer, agent, or anyone appointed by the

commission, is misconduct (Telecommunications Act. s. 85).
Generally, privileged communications, such as the communications between a doctor and his patient, or an advocate and his client, cannot be used as evidence in the courts but has been allowed by the Telecommunications (Amendment) Act (2006) (Telecommunications (Amendment) Act. ss. 97A, 97B and 97C). A writ petition was filed against this provision in the Supreme Court of Bangladesh, and the Supreme Court issued rules against such amended provision. The hearing on the writ petition is still pending, and the government did not yet reply to the rules (Karim, 2020).

This context generally signifies that the policymakers of Bangladesh are not much more respectful of citizens' right to privacy since the amended Telecommunications Act (2006) allows law-enforcing authorities to exercise unrestrained power to record telephone conversations of the individuals. Eventually, telecommunication privacy is under tremendous threat in Bangladesh due to, among others, the lack of adequate legal safeguards against the intrusion upon private communications.

Cybersecurity Laws

The major cybersecurity-related laws of Bangladesh, such as the Information and Communication Technology Act (2006) (the ICT Act), the Right to Information Act (2009) (the RTI Act), and the Digital Security Act (2018) (the DSA), contain some isolated privacy provisions.

The Information and Communication Technology Act (2006) is an omnibus enactment in Bangladesh to deal with chiefly e-commerce and cybercrime prevention-related issues, though lost its utility considerably due to the adoption of the DSA (2018), and deletion of some of its sections (54, 55, 56, 57, and 66) by the DSA.[3] However,

[3] The stated sections of the Information and Communication Technology Act 2006 were deleted by Section 61 of the Digital Security Act, 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

the ICT Act also contains some privacy-protective provisions. For instance, the enactment prescribes different kinds of punishments for the unlawful retention of electronic records; access to computers and data; failure to maintain books of accounts or records; unauthorised access to protected systems; and disclosure of confidentiality and privacy (ICT Act. ss. 9, 30, 50, 61, and 63). Moreover, to ensure enforcement issues, the ICT Act requires to set up 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 (ICT Act. ss. 68 and 82).

The Right to Information Act (2009) imposes some privacy obligations on diverse public sectors while enabling citizens to receive information from them. Given that the enactment ensures one particular right to the data subject, e.g., 'the right of access', it does not allow citizens the right to rectify the information about them (Greenleaf, 2014). It is noteworthy that receiving information under the RTI Act is not unrestrained, but rather restricted on several grounds. For example, the provisions of this enactment shall not apply to several institutions or organisations, which deal with the State security and intelligence specified in the Schedule thereof.[4] Furthermore, 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, or endanger the life, or physical safety of any person (ICT Act. ss. 7(h) and 7(i)). Besides, the law does not allow the disclosure of any information that is shared to any law enforcing body in confidence, or any legally protected confidential information (ICT Act. ss. 7(j) and 7(r)).

Subsequently, the government of Bangladesh passed the Digital Security Act (2018) to respond to long-term public demand for enacting a data privacy law, which came into effect on 8 October 2018. Now, the question is whether the provisions of this enactment are enough to ensure citizens' right to privacy.

[4] See Right to Information Act (2009). s. 83. As per the Schedule, the agencies that deal with the State security and intelligence, include: (1) National Security Intelligence (NSI); (2) Directorate General Forces Intelligence (DGFI); (3) Defence Intelligence Units; (4) Criminal Investigation Department (CID) of Bangladesh Police; (5) Special Security Force (SSF); (6) Intelligence Cell of the National Board of Revenue; (7) Special Branch, Bangladesh Police; and (8) Intelligence Cell of Rapid Action Battalion (RAB).

Although Section 2 of the Act contains some provisions, such as 'data storage', and 'illegal entrance', which are indirectly related to data privacy, there is no definition of major data protection-related phrases, such as 'personal data', 'sensitive personal data', 'processing', 'profiling', 'pseudonymisation', 'data subject', 'controller', 'processor', 'consent', 'supervisory authority', 'cross-border processing' etc., in clear terms.

The definition of 'Identity Information', as incorporated in Section 26, contains, *inter alia*, the name, address, date of birth, mother's name, father's name, signature, national identity, birth and death registration numbers, 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, iris image, and DNA profile of a data subject. Nevertheless, it cannot be considered as a proper definition of personal data because of the following reasons: (1) personal data must be with regard to a natural person only, not applicable to other legal entities, such as foundations, institutions, and corporations, or systems, but they are covered by the DSA (2018); (2) in the said definition of 'Identity Information', there is no reference for location data, 'IP address', 'website browsing history', or sensitive data, which are generally covered by the explanation of personal data in major data protection laws across the globe.

All the same, the enactment incorporates the provisions of punishments for numerous crimes having connections with data privacy. These include, *inter alia*, the unlawful access or damages to vital information infrastructures, digital devices, computers, or computer systems; deliberate access to any computers, Internet networks, or databases that may affect the friendly relationship with a foreign state, or goes against public order, or benefits a foreign state; 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; and unlawful entry into a computer or digital system, or unlawful assistance in the collection, or transfer of any information of a government, semi-government, autonomous, statutory body, or financial or commercial organisation (DSA. ss. 17-19; 27(1)(d); 32 and 33).

Besides, the DSA (2018) does not include numerous important 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; transborder data transfer issues; data protection principles; independent supervisory authorities, and effective enforcement mechanisms. Despite having some aspects of data privacy laws, the DSA (2018) can never be treated as an omnibus data protection law. Accordingly, the DSA 2018 cannot outweigh the utility of enacting a data protection law due to the abovementioned lapses.

Case Laws

Privacy is not a much-discussed topic in Bangladesh, although the citizens thereof experience diverse privacy dilemmas in many spheres of national life. Nonetheless, in the last few years, privacy appeared at the core of intellectual discourses due to the constant focus thereon by many scholars from different disciplines and the media. Moreover, in many cases, the judges refer to diverse aspects of privacy either in the form of ratio decidendi or obiter dicta.

In *Advocate Manzill Murshid and others v Bangladesh* (2011), the High Court Division of Bangladesh Supreme Court held, quoting from Lord Denning (1949), that it is a challenging job for the judges to strike the balance among different competing interests, such as the fair trial, personal freedom, property rights, non-retrospectivity, and privacy as opposed to the State power. However, in numerous cases, the Bangladeshi judiciary recognises some special aspects of privacy, such as (a) privacy of home; (b) privacy of correspondence and communication; (c) women's right to privacy and bodily integrity; and (d) financial data privacy.

(a) Privacy of home

In several case laws, the privacy of the home has been referred to as well as recognised in Bangladesh. In *Dr Ismat Mirza and other v Md Mosaddek Hossain and Ors* 7 BLC 90 1893, the plaintiff claimed in a partition suit that if the Court allows the defendant's portion to a stranger, it will infringe her privacy right. By analysing the circumstantial evidence, the Court observed that 'the claim of the plaintiff as for the infringement of privacy does not make any sense'. However, the privacy of the home has been recognised in numerous subsequent cases.

For example, in the *Government of Bangladesh and Others v Hussain Mohammad Ershad* (2000), it was held that every person shall have the right to be secure in his home as against any entry, search, and seizure as guaranteed in Article 43 of the Constitution. Similarly, in *Abdus Sobhan v Jamiruddin Jaigirder and Ors*. (1988), Justice Abdul Bari Sarker affirmed that privacy of home or private life is recognised as a customary easement right under Section 18 of the Easement Act (1882).[5] To recognise the privacy of the home, Justice Sarkar also referred to the provisions of Section 4 of the Partition Act (1893). Section 4 of the said enactment 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.

In *Sreemati Sobita Rani Bonik v Sree Gouranga Prasad Acharjee and Ors*, 17 BLT (HCD) 470, the High Court Division of the Supreme Court of Bangladesh explained, 'the very purpose of Section 4 of the Partition Act 1893 is to protect and preserve the sentiment of the co-sharers and attachment to their ancestral property, and also preserve the privacy of the members of the undivided family'. It is argued in several other cases[6] that by incorporating Section 18 of the Easement Act, the legislators intended to preserve the 'privacy of the members and inmates of the undivided dwelling house'. Similarly, in *Amena Khatun and others v Md. Afsaruddin* (1997), it was argued that 'the stranger purchaser, not acceptable to other members of the family, cannot reach to an undivided dwelling house, and possesses it forcibly'.

---

5 Illustration (b) of Section 18 provides that, by the custom of a certain town, no owner or occupier of a house can open a new window therein so as substantially to invade his neighbour's privacy.

6 *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.

(b) Privacy of correspondence and communication

Together with the privacy of the home, the privacy of correspondence and communication is also recognised by case laws. The precise facts of a case, *Imtiazur Rahman Farooqui (Md.) (MI Farooqui) v Bureau of Anti-Corruption and Others* (1998), reveal that the petitioner, a senior lawyer of Bangladesh Supreme Court, was asked to submit, *inter alia*, the information containing the names and addresses of all clients and all case numbers dealt by him during the period from 1-3-93 to 20-3-94. Justice Mainur Reza Chowdhury remarked that seeking information in this way was an errant nature targeting fishing activity towards one's information, and harassment to the petitioner, and accordingly, illegal. By the decision of the abovementioned case, it can be argued that among others, the privacy of correspondence and communication has been explicitly recognised in Bangladesh through case laws.

(c) Women's right to privacy and bodily integrity

The rights for women, including equality, liberty, freedom, or empowerment, may become meaningless unless protected by the privacy shield. It is also argued that if equality and freedom are such rights that each person must be entitled to, privacy is one of the crucial enablers by which one can access those rights (Vakharia, 2019). Therefore, together with other rights, women's privacy interest is also acknowledged by several case laws.

In Bangladesh, the forceful imposition of dress codes in favour of anyone whatsoever is prohibited and as such a punishable offence. For instance, in *Advocate Md. Salahuddin Dolon v Government of Bangladesh and Others* (2010), the High Court observed that an arbitrary imposition of gender-based dress codes outrage the right to privacy and women's right and freedom of expression protected under the international law. Being an active party to ICCPR, Bangladesh cannot disregard any provision of privacy laid down in different articles of the instrument (ICCPR. art. 2, 17, 19).

Furthermore, in *Bangladesh National Women Lawyers Association (BNWLA) v Bangladesh and others* (2009), a petition against the 'eve-teasing', the High Court Division of Bangladesh Supreme

Court stressed on several legal and constitutional rights of women,[7] including women's privacy, modesty, and secrecy as guaranteed by section 509 of the Penal Code (1860).

In *State v Mostafizur Rahman and another* (2013), Justice Imman Ali, while giving a dissenting judgment referring to the findings of an Indian Supreme Court case,[8] observed that by definition, rape is manifestly a violation of the right to privacy of women. In another case, *State v Secretary, Ministry of Law, Justice and Parliamentary Affairs and others case* (2009), Justice Imman Ali, while commenting on a child rape victim, remarked that Parliament should enact a robust law to save children from this persecution; support the victim and witness; ensure effective prosecution of offenders; and maintain confidentiality, privacy, and dignity of women.

Whereas in *Bangladesh Society for the Enforcement of Human Rights (BSEHR) and Others v Government of Bangladesh and others* (2000), Justice Md. Fazlul Karim remarked, 'we should bear in mind that nobody can violate the privacy of the inmates of any premises, or trespass it except in accordance with the law'. Justice Mr Karim pronounced this judgement observing the failure of police in protecting the privacy rights of sex workers.[9]

(d) Financial data

Financial data is always regarded as one of the most important personal data, and thus, requires strict legal protections. Nonetheless, in *Tarique Rahman v Director-General, Bureau of Anti-Corruption* (1999), the High Court Division of the Supreme Court of Bangladesh observed that:

---

7 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 in Article 31, and right to life and personal liberty, as ensured by Article 32 of the Constitution of Bangladesh (1972).

8 *Md. Iqbal v State of Jharkhand* (2013) AIR SC 3077.

9 On 23 July 1999, being directed by the district administration, police evicted some sex workers from their residence, Tanbazar, Nimtali, and Narayanganj, and took them to the Kashimpur Vagrant Home in the name of rehabilitation but physically abused the private parts of their bodies.

> 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.[10]

Perceivably, there should be specific legal protection for ensuring the secrecy in financial data, and that was recognised in a subsequent case. In *Badiul Alam Majumdar v Information Commission*, *Bangladesh* (2015), the petitioners asked to have the financial statements of the political parties but was denied by the Information Commission. The Information Office referred to the statements as confidential information of the third parties, and accordingly, they denied providing such information to the petitioners.

Conversely, in *Bangladesh & Ors v BLAST & Ors*. (2003) case, Justice Mr Kazi Md. Ejarul Haque Akondo dismissed the claim of the Information Commission that they have no lawful authority of holding the financial statements of the political parties by terming them as confidential. He further stressed that the annual financial reports of the political parties are neither any confidential nor any secret reports, but rather, these reports should be disclosed for demonstrating transparency, accountability, and building a clean image of the political leaders to the people.

ASSESSING PRIVACY REGIME

In the absence of a globally accepted criterion, evaluating the privacy protection regime of a particular jurisdiction is not easy. Nonetheless, by several tests, such as (1) definition, (2) contextual analysis, (3)

[10] Article 35(4) affirms that 'no person accused of any offence shall be compelled to be a witness against himself'.

privacy principles, and (4) enforcement mechanisms, the standard of a data protection regime can be tested.[11]

Definitional Test

By definitional test, it generally asks whether a particular legal regime possesses any law that can be termed as the data protection law by definition. The phrase 'data protection' refers to 'the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others'.[12] In contemporary Europe, if the data protection regime of a member nation complies with the standards, established by the GDPR, it can be assumed to have an adequate data protection regime. There is neither any such standard in Asia nor any universally accepted consensus about the minimum standard like the EU, by which the data protection regime of Bangladesh can be assessed.

It is generally perceived that a country is said to have an adequate data protection regime if it has a comprehensive data privacy law containing a set of data privacy principles compatible with the minimum standard as set by the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines (1980), along with certain specific modes of officially backed implementation (Greenleaf, 2014). Bangladesh does not have any data protection law that can satisfy this minimum requirement. Despite having numerous isolated privacy provisions, Bangladesh holds an inadequate data protection regime. In particular, the privacy protection regime of Bangladesh is in a nascent stage due to, among others, the following reasons: lack of comprehensive legislation; isolated privacy provisions leading to the patchwork of legal rules; lack of adequate provisions; and non-compliance to international data protection standards.

[11] To assess the standard of the data privacy laws of Asia, these four tests have been offered by Professor Graham Greenleaf, which can also be applied to examine the adequacy of the privacy regime of Bangladesh. For details of these tests, see Greenleaf, *Asian Data Privacy Laws*. pp. 51–75.

[12] This definition was developed by Brandeis, Warren, and Prosser, and later codified by Alan Westin in 1967. See generally, Alan F. Westin, *Privacy and Freedom § 7* (Atheneum, 1967). See also, Fred H. Cate, 'Principles of Internet Privacy', *Connecticut Law Review* 32 (2000): 877.

Contextual Analysis

By 'contextual analysis', it is intended to know what kind of protection is ensured by contextual surroundings, such as the Constitution, treaty, human rights organisations, civil, criminal, and administrative laws, and self-regulation (Greenleaf, 2014). Although privacy is conditionally recognised in the Constitution of Bangladesh, these constitutional guarantees apply vertically to cover only the public sectors. For the treaty protection, it was held in *Dr Shipra Chowdhury and another v Government of Bangladesh and others* (2009) that despite being accessed or ratified by Bangladesh, the Courts do not enforce the provisions of international human rights instruments in Bangladesh unless they are implanted in the domestic laws.

In the questions of protection of the civil, criminal, and administrative laws, privacy interests are generally protected by the application of the common laws, though there are several civil cases in which this right has not been recognised.[13] However, there remains hardly any provision regarding self-regulation in major sources of Bangladeshi laws that contain privacy provisions. Moreover, there are no significant activities of any human rights organisations 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.

Privacy Principles

The third test is whether the provisions of any law of a particular jurisdiction satisfy at least the minimum standard of data privacy as set by the OECD Guidelines (1980). The OECD Guidelines offered eight core 'basic principles of national application', such as data quality principle, purpose specification principle, use limitation principle, openness principle, security safeguards principle, collection limitation principle, individual participation principle, and accountability principle (OECD Guidelines. part two, principles

[13] *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.

7–14). It is explicit that no law of Bangladesh includes such privacy principles that satisfy at least the minimum data protection standards. Therefore, the privacy regime of Bangladesh remains far away to be evolved as an adequate privacy protection regime.

Enforcement Mechanisms

Effective enforcement mechanisms may also be a guide in assessing the standard of a data protection regime. Though there is no consensus on the standard of enforcement mechanisms of the data protection laws, the norm of the GDPR can be the guide in evaluating the adequacy of a data protection regime. Given this, the privacy regime of Bangladesh remains so far from the minimum requirement of having an adequate data protection framework due to the non-existence of a specific data protection legislation. Moreover, in the absence of specific data protection legislation, raising questions on enforcement issues seems to be meaningless. Simultaneously, without having effective enforcement mechanisms, any attempt for the protection of privacy in the legal regime of Bangladesh would appear as a nightmare.

SUGGESTIONS AND RECOMMENDATIONS

This section offers four complementary suggestions and recommendations, which can help to reduce diverse privacy challenges. The proposed suggestions include, *inter alia*, promoting privacy education, ensuring transparency in surveillance practices, conducting privacy impact assessment, and enacting an omnibus data protection legislation.

Promoting Privacy Education

One of the challenges that are usually faced by each government while attempting to protect privacy right is low public awareness. An important way of introducing a culture of respect for the protection of privacy may be ensured by launching privacy education at different levels of national life. The United Nations Educational, Scientific, and Cultural Organisation (UNESCO), for instance, emphasises that starting from an early age, the Internet and media literacy shall have to be added to the entire education system as part of the core life skills, greater civic education, or human development studies

(Mendel, et al., 2012). Moreover, basic privacy education is essential nowadays not only for cybersecurity practices but also to raise safe digital citizens (Egelman et al., 2016).

Beyond these, the judiciary can play pivotal roles to infuse trust, security, and confidence by curbing diverse sorts of cyber threats, such as malware attacks, denial-of-service attacks, botnets, spam, privacy threats, identity theft, phishing, hacking, cracking, or attacking critical infrastructure, and strengthening cybersecurity by taking steps against those activities (Abdul Ghani, 2020).

Ensuring Transparency in Surveillance Practices

During the period of the Revolutionary War, the central focus of the privacy problem was just to become free from governmental invasions (Solove, 2006). In the course of time, the trend has increased across the globe, including Bangladesh. Any systematic government surveillance programme is not justified unless it is transparent and grounded on proper explanations (Rubinstein et al., 2014). Nevertheless, there is no well-equipped and comprehensive legislation in Bangladesh to regulate excessive surveillance practices. Therefore, the ongoing surveillance practices in Bangladesh fall short of transparency holding ill-defined accountability measures. Such practices create suspicion and distrust among ordinary citizens. In such a context, it is essential to place the unregulated surveillance practices into a specific legal framework that outlines the power of law enforcing bodies, sets oversight compliance mechanisms, and renders available remedies to the victims.

Conducting Privacy Impact Assessments

Conducting a privacy impact assessment (PIA) is another crucial mechanism that may reduce the risks as caused by inadequate laws or lawlessness. PIA refers to a systematic process for evaluating the potential effects on the privacy of a project, initiative, proposed system, or scheme (Clarke, 2009). PIA generally works as an 'early warning system' for both government agencies and businesses to make better-informed decisions by avoiding the privacy disaster before launching any scheme. A PIA regime can save government entities, businesses, or other stakeholders from possible damages that might have been caused on privacy grounds. A PIA report has the potential to save both

money and reputation (Office of the Privacy Commissioner, 2007). In connection with tremendous threats to privacy, excessive surveillance practices, and privacy-unfriendly laws, PIA should be conducted to evaluate the probable privacy implications in the current legal regime of Bangladesh.

Enacting Data Protection Legislation

It has become explicit that Bangladesh holds an inadequate privacy protection regime mostly due to the lack of comprehensive data privacy legislation. Therefore, paying heed to all other measures, Bangladesh should immediately enact a comprehensive data privacy law. A sound data protection legislation is important for the protection of fundamental human rights and the right to privacy (Vanberg, 2021). The enactment is also important to set an autonomous body for monitoring the entire data protection regime while assessing their impacts, and carrying out other initiatives required for implementing the legal rules (Yilma, 2015).

In the question of a model, Bangladesh may enact a GDPR-styled data protection legislation. The GDPR emerges as the standard for the global data protection regulations being facilitated by its omnibus legal substance, extensive extraterritorial scope, and the influential market powers of the EU (Islam & Karim, 2020b). Therefore, it is claimed that 'the GDPR' appears as a clarion call for a unique global data privacy gold standard (Buttarelli, 2016). It is noticed that there is an unprecedented wave of enacting GDPR-styled data protection laws across the globe. Schwartz (2019) rightly observed that:

> EU data protection law is playing an increasingly prominent role in today's global technological environment. The cornerstone of EU law in this area, the General Data Protection Regulation (GDPR), is now widely regarded as a privacy law not just for the EU, but for the world (Schwartz, 2019).

CONCLUSION

Privacy is one of the most desired human rights in this era of ubiquitous computing when diverse activities are going online using

personal data. In the last few decades, governments, businesses, and other private entities have been processing large-scale personal data for numerous purposes, but mostly without the knowledge of the persons concerned. This landscape poses tremendous challenges to privacy, and eventually, privacy appears as one of the hot-button issues in contemporary global politics, policies, and business (Islam & Karim, 2019a), and Bangladesh is not an exception.

In response to these ever-growing challenges, numerous policy measures have been adopted at national, regional, and international levels. At the domestic level, a total of 145 countries have already passed data privacy laws across the globe, while many other nations are attempting to amend their relevant laws (Greenleaf, 2021). The people of Bangladesh are also experiencing various privacy dilemmas due to, among others, the national ID card preparation scheme; biometric SIM registration scheme (Ahmed SI et al., 2017); excessive surveillance practices; anti-terrorism movements, and some other reasons, including e-commerce; social media; and ride-sharing apps. Accordingly, the people of Bangladesh, like the citizens of countries with omnibus data protection laws, deserve to have adequate legal protections against such privacy invasions.

This backdrop requires extensive research to explore whether there are any legal provisions for the protection of privacy and personal data in the legal regime of Bangladesh. If there is any, to what extent such legal protections are adequate in comparison with global data privacy standards. Nonetheless, such kind of legal research is lacking in the existing literature. This research aims to fulfil the gap by using doctrinal, or desk-based, or library-based research methodology.

The findings of this study revealed that despite the lack of comprehensive privacy or data protection legislation in Bangladesh, privacy is conditionally recognised in the Constitution of Bangladesh. Moreover, there are numerous isolated privacy provisions in many subsidiary laws, and diverse aspects of privacy have been recognised in many case laws of the country. Nevertheless, Bangladesh maintains an inadequate privacy protection regime due to, *inter alia*, lack of comprehensive legislation; isolated privacy provisions leading to the patchwork of legal rules; lack of adequate provisions; and non-compliance to the international data protection standards. To overcome this situation, this paper suggests for the policymakers of Bangladesh

to consider the following four policy measures, such as fostering privacy education; ensuring transparency in surveillance practices; conducting privacy impact assessments; and finally enacting an omnibus data protection legislation.

ACKNOWLEDGEMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Abdul Ghani, A. I. M. (2020). Challenges for legal education in the era of I.R.4.0. *UUM Journal of Legal Studies*, *11*(2), 27–51. https://doi.org/10.32890/uumjls. 11.2.2020.7731

Abdus Sobhan v Jamiruddin Jaigirder and Ors. (1988) BLD 257.

Advocate Manzill Murshid and others v Bangladesh. (2011). 40 CLC (HCD).

Advocate Md. Salahuddin Dolon v Government of Bangladesh and Others. (2010). 39 CLC (HCD) [3765] 63 DLR (HD) (2011) 80.

Ahmed, S. I., Haque, M. R., Guha, S., Rifat, M. R., & Dell, N. (2017, May). Privacy, security, and surveillance in the global south: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, May 2017 (pp. 906–918).

Amena Khatun and others v Md. Afsaruddin. (1997). 26 CLC (HCD) [6339]/ 50 DLR (HCD) (1998) 156.

Ayub, Z. A., & Yusoff, Z. M. (2020). Right of online informational privacy of children in Malaysia: A statutory perspective. *UUM Journal of Legal Studies*, *9*, 2020.

Badiul Alam Majumdar v Information Commission, *Bangladesh.* (2015). 69 DLR (HCD) 100, Writ Petition No.798.

Bangladesh & Ors v BLAST & Ors, 55 DLR. (2003). 363.

Bangladesh Computer Council. (2019). *e-Government Master Plan for Digital Bangladesh*. https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/publications/3f9cd471_9905_4122_96ee_ced02b7598a9/2020-05-24-15-54-43f3d2b8b4523b5b62157b069302c4db.pdf

Bangladesh National Women Lawyers Association (BNWLA) v Bangladesh and others. (2009). 14 BLC (2009) 694.

Bangladesh Society for the Enforcement of Human Rights (BSEHR) and Others v Government of Bangladesh and others. (2000). 29 CLC (HCD) [3662]/ 53 DLR (2001) 1.

Bangladesh Telecommunications Act, Act No. 18. (2001).

Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation and Governance*, *14*(3), 447-464.

Bennett, C., & Oduro Marfo, S. (2019, October). Privacy, voter surveillance and democratic engagement: Challenges for data protection authorities. In *Proceedings of International Conference of Data Protection and Privacy Commissioners (ICDPPC)*, October 2019. Retrieved from https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf

Buttarelli, G. (2016). The EU GDPR as a Clarion call for a new global digital gold standard. *International Data Privacy Law*, *6*(2), 77.

Calhoun, J. B. (1950). The study of wild animals under controlled conditions. *Annals of the New York Academy of Sciences*, *51*(6), 1113–1122.

Castells, M., Blackwell, C. J. E., Planning, P. B., & Design. (1998). The information age: Economy, society and culture. Volume 1. The Rise of the Network Society. *25*, 631–636.

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law and Security Review*, *25*(2), 123.

Code of Civil Procedure, Act No. 5. (1908).

Code of Criminal Procedure, Act No. 5. (1898).

Constitute. (2021). *Constitutions.* https://www.constituteproject.org/search?lang=en&key=privacy

Constitution of the People's Republic of Bangladesh, President Order No. 76. (1972).

Cooley, T. M. (1930). *A treatise on the Law of Torts* (Vol. 2). Callaghan.

de Hert, P., & Schreuders, E. (2001). *The relevance of Convention 108' 33, 42: Proceedings of the Council of Europe Conference on Data Protection*, November 2001, Warsaw: Poland.

Denning, A. T. D. (1949). *Freedom under the law*. London: Stevens.

Digital Security Act, Act No. 46. (2018).

Dispute Resolution (Municipal Area) Board Act), Act No. 12. (2004).

Dr Shipra Chowdhury and another v Government of Bangladesh and others. (2009). 38 CLC (HCD) [9178] = 29 BLD (HCD) (209) 183.

Easement Act, Act No. 5 (1882).

Egelman, S., Bernd, J., Friedland, G., & Garcia, D. (2016, February). The teaching privacy curriculum. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education* (pp. 591–596).

Elison, L. M., & NettikSimmons, D. (1987). Right of privacy. *Montana Law Review*, *48*(1), 1.

Family Courts Ordinance, Ordinance No. 18. (1985).

Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law and Security Review*, *29*(5), 522–530.

Government of Bangladesh and Others v Hussain Mohammad Ershad. (2000). 52 DLR (AD) 162.

Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. OUP Oxford.

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, *69*, 1, 3–5.

Imtiazur Rahman Farooqui (Md.) (MI Farooqui) v Bureau of Anti-Corruption and Others. (1998), 27 CLC (HCD)[7457]/ 51 DLR (HCD) (1999) 421.

Information and Communication Technology Act, Act No. 39. (2006).

Islam, M. T. (2018). Abu Bakar Munir, Siti Hajar Mohd Yasin and Ershadul Karim. Data protection law in Asia. *International Data Privacy Law*, *8*(4), 338–340.

Islam, M. T., & Karim, M. E. (2019a). A brief historical account of global data privacy regulations and the lessons for Malaysia. *SEJARAH: Journal of the Department of History*, *28*(2).

Islam, M. T., & Karim, M. E. (2020b). Extraterritorial application of the EU General Data Protection Regulation: An international law perspective. *IIUM Law Journal*, *28*(2), 531–565.

Islam, M. T., Munir, A. B. & Karim, M. E. (2021). Revisiting the right to privacy in the digital age: A quest to strengthen the Malaysian data protection regime. *Journal of Malaysian and Comparative Law*, *48*(1), 49–80.

Karim, M. (2020). *Cyber law in Bangladesh*: Wolters Kluwer, Netherlands.

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law and Security Review*, *25*, 309.

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., & Torres, N. (2012). *Global survey on Internet privacy and freedom of expression.* UNESCO.

Mirshekari, A., Ghasemi, R., & Fattahi, A. (2020). Digital accounts after death: A case study of Iranian law. *UUM Journal of Legal Studies*, *11*(2), 153–182. https://doi.org/10.32890/uumjls.11.2.2020.7505

Moore, A. D. (2003). Privacy: Its meaning and value. *American Philosophical Quarterly*, *40*(3), 215.

O'Connor, N. (2018). Reforming the US approach to data protection and privacy. Council on Foreign Relations, 30.

OECD. (1980). OECD guidelines on the protection of privacy and transborder flows of personal data.

Office of the Australian Information Commissioner. (2021). What Is privacy? https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy/#:~:text=Privacy%20is%20a%20fundamental%20human,well%20as%20freedom%20from%20discrimination.andtext=Generally%20speaking%2C%20privacy%20includes%20the,freely%20with%20whom%20you%20want

Office of the Privacy Commissioner, Wellington, New Zealand (2007). Privacy impact assessment handbook. https://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf

Orwell, G. (2009). Nineteen eighty-four: Everyman's Library.

Partition Act, Act No. 4. (1893)

Penal Code, Act No. 45. (1860).

Penenberg, A. L. (2001). The surveillance society learning to love the end of privacy. WIRED-San Francisco, 9(12), 156–161.

Posner, R. A. (1977). The right of privacy. Georgia Law Review, 12, 393.

Privacy International. (23 October 2017). What Is privacy? https://www.privacyprivacyinternational.org/explainer/56/what-privacy

Right to Information Act, Act. No. 20. (2009).

Rouvroy, A., & Poullet, Y. (2009). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In Gutwirth, S. and others (Eds.), Reinventing data protection? (p. 70). Springer: Dordrecht.

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: A comparative analysis. International Data Privacy Law, 4(2), 96–119.

Schwartz, P. M. (2019). Global data privacy: The EU way. New York University Law Review, 94.

Simitis, S. (1987). Reviewing privacy in an information society. University of Pennsylvania Law Review, 135(3), 707–709.

Sivarasa Rasiah v Badan Peguam Malaysia & Anor case, 2 AMR 301 (2010) 2 MLJ 333.

Solove, D. J. (2006). A brief history of information privacy law in Proskauer on privacy, PLI. GWU Law School Public Law Research Paper No. 215. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271

State v Mostafizur Rahman and another. (2013). 42 CLC (AD) [9154]/ 67 DLR (AD) (2015) 218.

State and Ors v Oli and Ors. (2019). LEX/BDHC/0128/2019 (Death Reference no. 61 of 2011 & Criminal Appeal no. 6592 of 2011).

State v Secretary, Ministry of Law, Justice and Parliamentary Affairs and others case (2009) 38 CLC (HCD) [5300] = 30 BLD (HCD) (2010) 369; 15 MLR (HCD) (2010) 59.

Syed Nong, S. N. A., Mustaffa, A., Ismail, N., Salleh, K., Yusof, M. N., & Awang, M. B. (2020). Protection of children beyond control in the IR 4.0 era: The role of international conventions. UUM Journal of Legal Studies, 11(2), 77–96. https://doi.org/10.32890/uumjls.11.2.2020.8695

Tarique Rahman v Director-General, Bureau of Anti-Corruption. (1999). 28 CLC (HCD) [4709]/ 52 DLR (2000) 518.

Telegraph Act, Act No. 13. (1885).

Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. International Data Privacy Law, 3(2), 88–90.

UNCTAD. (United Nations). (2016). Data protection regulations and international data flows: Implications for trade and development. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

United Nations. (1948) Universal declaration of human rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). International covenant on civil and political rights.https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Vakharia, P. (2019). Unveiling privacy for women in India. Law Review Government Law College, 10, 37.

Vanberg, A. D. (2021). Informational privacy post GDPR–end of the road or the start of a long journey? The International Journal of Human Rights, 25(1), 52–78.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193.

Westin, A. F. (1967). Privacy and freedom (Vol. 7). New York: Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 27.

Wireless Telegraphy Act, Act No. 17. (1933).

Yilma, K. M. (2015). Data privacy law and practice in Ethiopia. International Data Privacy Law, 5(3), 189.