A RESEARCH PAPER ON

Protection of Biometric Data: A Comparative analysis in relation with Right to Privacy Law between India, UK, USA and Bangladesh.

COURSE TITLE: SUPERVISED DISSERTATION

COURSE CODE: LAW 406

DEPARTMENT OF LAW

EAST WEST UNIVERSITY

SUBMITTED TO

SAYEED HOSSAIN SARWAR

LECTURER, DEPERTMENT OF LAW

EAST WEST UNIVERSITY

SUBMITTED BY

JOYETA HASAN ROJA

ID: 2017-3-66-007

DATE: 22-05-2022

TOTAL WORD COUNT: 6784

Consent form

Consent Form

The dissertation titled: Protection of Biometric Data: A Comparative analysis in relation with Right to Privacy Law between India, UK, USA and Bangladesh.

Prepared by: Joyeta Hasan Roja. ID : 2017-3-66-007. Submitted to:

Sayeed Hossain Sarwar for the fulfillment of the requirements of Course 406 (Supervised Dissertation) for LL.B. (Hons.) degree offered by the Department of Law, East West University is approved for submission.

.....

Signature of the Supervisor

Date: 22.5.2022

“ACKNOWLEGMENT”

Initially, I am pleasing appreciating to my almighty. Exclusive of his support, I was not able to complete this research paper. I moreover would like to appreciations to East West University for permitting me the chance to conduct this research paper.

However, I also would like to give my special thanks to my respective and cooperative faculty for their supportive guidance. I will not ever forget all the significant advice which my teachers gave me during the research. I am also pleased with my parents, elder brothers and sisters, who aided me a lot in managing my research paper. My father contributed a lot of motivation and my mother provided me with inspiration at the time of my research paper.

Though, my elder brother who was also always with me and my sisters gave me motivation and contributed to my recommendation to conduct my research properly.

Finally, I was able to comprehensive my research effectively. Though it was not easy to work on, I finished my research paper with lots of knowledges, which gave me inspiration for my future life.

“DECLARETION”

I, **Joyeta Hasan Roja,** bearing **Student Id- 2017-3-66-007** hereby solemnly declare and affirm that I have done this research task and that the entire or limited portion of this research paper has not been submitted or published by any journal or any newspaper or any article. I have entirely created this Dissertation paper and the materials is used for this research paper has been accredited properly, and a list of footnotes and references has been provided.

.....

(Joyeta Hasan Roja)

ID:2017-3-66-007

L.L.B (Hons), East West University

ABSTRACT

The development of biometric technology is the latest technologies of unique identification. The citizens of every country in the world are used to this exceptional identification technology for their authentication safety. The aim of this research paper is to compare the law and rules of the protection of biometric data in relation to right to privacy in UK, USA, India and Bangladesh. Biometric technology is entirely depending on personal data i.e., facial scan, fingerprint scan, eye scan and so forth. Personal data is violated by using technology in every step. So, violation of personal data would be considered as violation of right to privacy. Hence, this research paper, as I previously mentioned is to compare the protection of biometric data in relation to right to privacy in UK, USA, India and Bangladesh respectively. Therefore, the law and regulation of the said countries are also discussing in this research paper. The finding of this research paper is to comparative analyses of legal framework of the protection biometric data in relation to the right to privacy in abovementioned countries. While doing this research paper, it will find that the finest legal framework exercise of the protection of biometric data in relation to right to privacy among the aforementioned countries, it will find that UK has the best legal framework by practicing UK General Data Protection Regulation (GDPR). This is because, the protection of biometric data in relation to right to privacy is well respected and protected in UK among USA, India and Bangladesh. In UK they are ensuring the protection of biometric data in relation to right to privacy through the comprehensive protection of biometric data in relation to right to privacy law i.e., UK GDPR. However, in USA, they have not any comprehensive law of protection of biometric data

in relation to right to privacy. For this reason, the states of USA rely on the Biometric Information Privacy Act, since 2008, which was firstly passed by the Illinios state among 50 states of USA. Many states i.e., Taxes, Washington and so forth in USA are incorporating their protection of biometric data in relation to right to privacy in light of BIPA. This is because, BIPA provides the comprehensive legal framework of the protection of biometric data in relation to right to privacy. In India, they did not recognise the right to privacy law as fundamental rights, but after the pronouncement of Aadhaar[1] case, the Supreme Court of India recognised the protection of biometric data in relation to right to privacy as fundamental right by amending Section 57 of the Aadhar Act 2016[2]. Consequently, in Bangladesh the right to privacy is guaranteed under Article 43 of the Constitution of Bangladesh as fundamental right. However, Bangladesh did not legislate or recognise any law for the protection of biometric data in relation to right to privacy. Therefore, the finding of this study is that the developing countries i.e., Bangladesh and India can legislate new rules and law in light of UK GDPR for the protection of biometric data in relation to right to privacy.

Keywords: Biometric system, Data protection and data collection, right to privacy, Security, Laws.

[1] Aadhaar means 12-digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India.

[2] Section 57 of Aadhaar Act, 2016, that authorize the application of the 12-digit Aadhar number for the identification of a citizen in India for any purposes- whether by the State or any cooperate or person.

ABBREVIATION

BIPA: Biometric Information Privacy Act 2020.

CCPA: California Consumer Privacy Act of 2018

DPA Act 2018: UK Data Protection Act 2018.

(DPO): Data Protection officer.

(DPIAs): Data Protection Impact Assessments

DSA: Digital Security Agency.

DSA: Digital Security Act

EU: European Union

FIPPs: fair data practice standards.

(GDPR): General Data Protection Regulation

ICT Act: *Information and Communication Technology Act*.

NDSC: National Defense and Security Council.

RTI: Right to Information Act.

Table of Contents

COVER PAGE. **1**

ACKNOWLEGMENT **2**

DECLARETION **3**

ABSTRACT **4**

ABBREVIATION **6**

TABLE OF CONTENTS **7**

CHAPTER 1: INTRODUCTION. **10**

1.1 Background **10**

1.2 Objective of the Research **11**

1.3 Methodology **11**

1.4 Limitation **12**

1.5 Research Question **12**

CHAPTER 2: PROTECTION OF BIO MATRIC DATA IN PRIVACY REGIME. **13**

2.1. Introduction **13**

2.2 What is Biomatric Data **13**

2.3 Biometric Data and the Right to Privacy **14**

2.4. Conclusion. **15**

CHAPTER 3: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN UK. **16**

3.1. Introduction. **16**

3.2. Background on Biometric Data Protection in UK. **16**

3.3 Key Legislation's of UK **17**

3.3.1. UK GDPR **17**

3.3.2. Data Protection Act 2018 (DPA) and Data Protection Officer (DPO) **18**

3.4. Conclusion. **18**

CHAPTER-4: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN USA. **19**

4.1. Introduction **19**

4.2. The Illinois Biometric Information Privacy Act (BIPA). **19**

4.3. Current dispute State Biometric Privacy Status (Patel v Facebook, Inc). **20**

4.4. Conclusion. **21**

CHAPTER-5: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN INDIA. **22**

5.1. Introduction **22**

5.2. Regulation of Biometric Data in India **22**

5.3. Biometric Data and Personal Data Protection Bill **23**

5.4. Use of Biometric Data, Post Aadhaar Period **24**

5.5. Conclusion **25**

CHAPTER-6: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN BANGLADESH. **26**

6.1. Introduction. **26**

6.2 Regulation of Biometric Data Protection and Law of Privacy in Bangladesh **26**

6.3. Data Protection Authority **27**

6.4. Conclusion **28**

CHAPTER-7: COMPARATIVE ANALYSIS OF OF PROTECTION OF BIOMETRIC DATA IN UK, USA, INDIA AND BANGLADESH. **29**

7.1. Introduction **29**

7.2. Comparative analysis of Protection of Biometric Data in relation to Right to Privacy in UK, USA, India and Bangladesh. **29**

7.3. Conclusion **31**

CHAPTER 8: CONCLUSION AND RECOMMENDATION

8.1 Conclusion **32**

8.2 Recommendation. **33**

BIBLIOGRAPHY **34**

Chapter 1: Introduction.

1.1 Background

These days biometric technology is progressively utilized for a wide scope of exercises going from personality confirmation to border line security, voting system, medical care, schooling, etc[3]. Apparently, biometric distinguishing proof frameworks are being utilized all over the world especially after the terrorist attack in the USA on September 11, 2011[4]. However, there is a tremendous privacy concern in the developing nations like Bangladesh and India. In Bangladesh and India legitimate shields i.e. acts of parliament and rules, to safeguard the right to privacy and data security are not satisfactory. The development of new technologies, for example, biometric technology is gradually noticeable[5].

In the present digital information environment, personal data protection is played a key role in biometric technology. The modern era of data and innovation or technology has transformed a person's personal data, which needs some protection[6]. This research paper will consider the comparative analysis regarding the data protection and the right to privacy law between UK, USA, India and Bangladesh respectively. In this context, the legal safeguard of the data protection and the right to privacy in the countries needs to be examined.

[3]Ibid.
[4]Chirchir, R.; Farooq, S. 2016. Single Registries and Social Registries: clarifying the terminological confusion, Pathways' Perspectives on social policy in international development, Issue No. 23, November 2016 Kent, United Kingdom, Development Pathways). Available at: http://www.developmentpathways.co.uk/resources/wpcontent/uploads/2016/11/Single-and-Social-Registries.pdf [05.05.2022].
[5]Kidd, S. 2011. Good practice in the development of management information systems for social protection. Pension watch Briefings on social protection in older age. Briefing no.5 (HelpAge International, London).
[6]*Dijkhoff, T.; LetlhokwaMpedi, G. (eds.). 2017. Recommendation on Social Protection Floors: Basic Principles for Innovative Solutions (The Netherlands, Kluwer Law International B.V.).*

1.2 Objective of the Research

The objective of this research paper is to explore the legal framework i.e., UK GDPR in UK, BIPA in USA, Aadhaar case in India and Digital Securities Act, 2018 in Bangladesh for protection of biometric data in relation to the right to privacy in UK, USA, India and Bangladesh.

1.3 Methodology

This research paper is based on the qualitative method of research, as it will evaluate or re-examine various factors that create the differences between the developed and developing countries. During conducting this research paper, the resources like statutes, international conventions and cases are contemplated as primary sources. Regarding the secondary resources, books and national and international journals, newspaper articles website, online journals, scholars' blogs are considered. On conducting this thesis paper some lack of resources has been identified and which will describe in limitation chapter.

1.4. Limitation

In conducting this research paper, lots of limitations were confronted. Among the limitations, limited access to the internet hindered the research on collecting resources. Due to the Covid-19 pandemic, it was not possible to access the university library and find the significant article, journal access, books, and statutes. Another limitation during this research is regarding my defective laptop, which obstructed my research. Without this limitation, this research would be more informative, organized, spontaneous and effective.

1.5 Research Question

1. What are the legal framework regarding protection of biometric data in relation to right to privacy in UK, USA, India and Bangladesh?

2. What is the best practice for the protection of biometric data in relation to right to privacy among the abovementioned countries?

CHAPTER 2: PROTECTION OF BIO MATRIC DATA IN PRIVACY REGIME.

2.1. **Introduction**

In recent years, identification through biometric data systems has become an essential practice given that this is the newest technology of unique identification. This is because; nowadays the people all around the world are using these systems for their safety and security. This chapter shall define the term biometric data and explore the link among protection of biometric data and the law of privacy respectively.

2.2 What is Biomatric Data

The term 'biometric data' can be recognized as the measurement and the statical analysis of a unique physical and behavioral characteristic of a human being. It is modern-day's technology which is mainly exercised for the identification of a person[7]. The basic objective of biometric data is to authenticate a person by his physical or behavioral characteristics which include thumbs expression, face recognition, and so forth. However, the basic principle of the biometrics data can be seen as the authentication of a human being perfectly and identifying the person by his physical and behavioral character. The said phrase is originated from the Greek term bio that signifies the life and metrics which signify the measure[8].

[7]*R. E. O. Paderes, A Comparative Review of Biometric Security Systems, Proc.- 8th Int. Conf. Bio-Science Bio-Technology, BSBT 2015, 8–11, 2016.*

[8]Troy Hunt: The 773 million Record 'Collection #1' Data Breach. [Online]. Available: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/. [Accessed: 26-Mar.-2022]

Biometric data frameworks are used to recognize or check the personality of individuals by utilizing their natural physical or behavioural conduct characters. These physical or behavioural characteristics are called biometric identification which includes, inter alia, fingerprints; face and palm prints; stride; voice; and DNA. The public authority collects that biometrics data sets can be utilized successfully.

2.3 Biometric Data and the Right to Privacy

The law of privacy was introduced by the American fourth amendment in the constitution of USA in 17th century and is exercised by all-around the world[9]. The legal definition of the right to privacy can be seen as the right of a person to be free from interference into or publicity regarding complications of a personal nature[10]. Article 12 of the Universal Declaration of Human Rights (UDHR) provides that "no one shall be subjected to arbitrary intervention with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. All has the right to the protection of the law beside such intervention or occurrences.[11]" The greatest problem of the biometric data arises in relation to the law of privacy comes from the public authority's capacity to involve it for observation. Further, geolocation following advances based on top of huge biometrics assortments could authorise consistent opinion. In this context, Security Council of the UN has published respective Resolutions on the collection of biometric data and allocation of the same for the purpose of counterterrorism. The Security Council Resolution 2160 (2014) encourages Member States to submit photos and additional biometric data of individuals associate

[9] US v Jones, 615 F. 3d 544.
[10] Ibid.
[11] 'The Right to Privacy' (Lawteacher.net, April 2022) <https://www.lawteacher.net/free-law-essays/human-rights/right-to-privacy.php?vref=1> accessed 19 April 2022

with the Taliban to INTERPOL"[12]. "Resolution 2322 (2016) extended the approval for biometric-related data sharing to terrorists and terrorist organisations in general"[13].

2.4. **Conclusion.**

Accordingly, biometric data would be considered as the information which is collected through biometric technologies i.e., facial recognition or fingerprint scanners. The information has to be collected for surveillance reasons, but in countries like UK and USA, biometric data have started applying as biometric tools for mass surveillance of the citizens. As a result, the uses of biometrics for surveillance or monitoring purposes are concerned with people's territorial privacy.

[12]Ibid.
[13]Ibid.

CHAPTER 3: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN UK.

3.1. Introduction.

UK has announced complete rules and regulation, which pursues to legalize data protection and protect the right to privacy of an individual respectively. The General data protection regulation (GDPR) and Data Protection Act 2018 are the current privacy and data protection regulation in the UK. The GDPR prohibits the processing of biometric data for the purpose of uniquely identifying natural persons. This chapter of this research paper looks at biometric data security and the law of privacy in the UK with the examination of the meaning of the term personal data and its protection in legislation terms.

3.2. Background on Biometric Data Protection in UK.

The progress of biometric data protection in UK followed since 1970s. In 1984 the Data Protection Act had been approved by the House of Commons. By the said Act, the UK parliament conveys subject access rights to personal information held on computerized records[14]. Subsequently, in the year 2000, the UK parliament passed its own Freedom of Information Act, 2000, and later, it was coming into force in 2005[15]. The data protection Act, 1984 was the Act of parliament concerning

[14]Future of Privacy Forum, "Mobile location analytics code of conduct," 2013 [Online]. Available: http://www.futureofprivacy.org/wp-content/uploads/10.22.13- FINAL-MLA-Code.pdf. (Acess on 02.05.2022).
[15] Ibid.

data security in the UK and it was developed because the term personal information is used by the government bodies[16]. However, the said Act was passed a generation ago[17].

3.3 Key Legislation's of UK

3.3.1. EU GDPR AND UK GDPR

In UK the key piece of legislation concerning data protection is GDPR. GDPR incorporates the Directive 95/46/EC[18] which is the data protection directive driving toward the expanded harmonization of the information assurance regulation all through the National Laws of EU Member States[19]. The obligation of EU General Data Protection Regulation (GDPR) was incorporated into UK legislation through Data Protection Act, 2018 on May 2018[20]. Subsequently, UK left the European Union (EU) on December 31, 2021 by Brexit and after Brexit, they are no longer regulated domestically by the EU's GDPR. Instead, the UK now has their own version of GDPR, known as UK-GDPR for their citizen, but for the citizen of EU, UK courts are still applying the EU-GDPR. The UK-GDPR took effect on January, 31, 2020[21]. The UK GDPR generally adopted all rules and regulation laid down in EU GDPR, except the UK GDPR changes key areas of the law concerning national security, intelligence service and immigration[22].

[16]L. Amoore, "Biometric borders: Governing mobilities in the war on terror," Political geography, Vol. 25, No. 3, pp. 336-351, 2006.
[17] Ibid.
[18] A legal instrument of the European Union (EU) as defined in Article 288 of the Treaty on the Functioning of the European Union (TFEU).
[19] New UK-GDPR law after Brexit | Compliance with Cookiebot CMP, Available at- https://www.cookiebot.com/en/uk-gdpr/ (Access on-10.05.2022).
[20]Information Commissioner's Office, 'Controllers and processors: What does it mean if you are a controller?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ controllers-and-processors/what-does-it-mean-if-you-are-a-controller> accessed 07 April 2012.
[21] New UK-GDPR law after Brexit | Compliance with Cookiebot CMP, Available at- https://www.cookiebot.com/en/uk-gdpr/ (Access on-10.05.2022).
[22] Ibid.

3.3.2. Data Protection Act 2018 (DPA) and Data Protection Officer (DPO)

The Data Protection Act, 2018 was introduced in the UK in the year 2018 in light of EU-GDPR. It contains specific restrictions and derogation of primary data protection. By the Act of 2018, the UK government introduced a Data Protection Officer (DPO) and his functions[23]. The task of DPOs is to assist in monitoring internal compliance, inform and advise on the protection of the biometric data obligations and act as a contact point for the protection of the biometric data in relation to the right to privacy[24].

3.4. Conclusion.

Accordingly, in UK, privacy and data protection is protected by the Article 8 of ECHR (European Convention on Human Rights). Therefore, in UK the right to data protection could be a precaution not only for privacy, but it can also protect the fundamental rights laid down in ECHR.

[23]Ibid.
[24] Ibid.

CHAPTER-4: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN USA.

4.1. Introduction

The law in relation to protection of biometric data in the USA mirror a typical arrangement of standards, every now and again alluded to as "fair data practice standards" or FIPPs[25] (fair data practice standards). Though FIPPs various protection regulations have developed in the USA. This chapter of this study will discuss the biometric data security and the right to privacy in the USA.

4.2. Biometric Information Privacy Act (BIPA).

As I mentioned earlier in USA, they have not any comprehensive law of protection of biometric data in relation to right to privacy. For this reason, the states of USA rely on the Biometric Information Privacy Act, since 2008, which was firstly passed by the Illinios state among 50 states of USA. Many states i.e., Taxes, Washington and so forth in USA are incorporating their protection of biometric data in relation to right to privacy in light of BIPA. This is because, BIPA provides the comprehensive legal framework of the protection of biometric data in relation to right to privacy. BIPA is unique in that it provides aggrieved parties with a private right of action. BIPA, is an Illinois resolution that directs the assortment, use, maintenance, and obliteration of people's biometric identifying data, for example, fingerprints, retina sweeps, and facial calculation examines[26]. The Illinois Legislature sanctioned BIPA to address the developing utilization of

[25]U.S. Federal Trade Commission (FTC), Privacy Online: A Report to Congress (1998), at 7, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf); Asia-Pacific Economic Cooperation (APEC), Privacy Framework (2005), https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-PrivacyFramework/05_ecsg_privacyframewk.pdf). Access on-08.04.2022.

[26] *Fisher, Sandra L. (2020). "Encyclopedia of Electronic HRM" (PDF). University of Twente Research Information System (RIS).*

biometric data by organizations to smooth out monetary exchanges and security screenings[27]. The reason for BIPA is to give unique security to such data, both to lessen the gamble of wholesale fraud and to urge people in general, to partake in biometric-worked exchanges[28]. BIPA applies extensively to any private element that works or carries on with work in Illinois (whether or not the substance is settled in Illinois). BIPA incorporates five key arrangements: Written Policy, informed assent, utilization, divulgence, and Security.

4.3. Current dispute State Biometric Privacy Status (Patel v Facebook, Inc).

Since the inception of the BIPA statute, there has been substantial development in case law. In this case, *Patel v Facebook Inc*[29] is a significant one. In Patel case, where the plaintiff brought an action against Facebook for BIPA violations[30] that Facebook's facial-recognition technology violated the provisions of BIPA. The Supreme Court of the USA in Patel case held that the improvement of the face templated using facial-recognition technology exclusive of consent invades of an individual's personal matters and existing interests. The panel of the Judges held that the lower court, in this case, did not misuse its consideration by confirming the class; the BIPA extraterritoriality law, which did not prevent the lower court from finding the majority; and the lower court did not misuse its consideration that a class of action was higher than individual actions[31].

[27] Ibid
[28] Michael Hintze, In Defense of the Long Privacy Statement, 76 MD. L. REV. 1044 (2017).
[29] *Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).*
[30] Ibid.
[31] Ibid.

4.4. Conclusion.

Accordingly, in 2008, Illinois became the principal state to determine a Biometric Information Privacy Act (BIPA). BIPA controls "the assortment, use, defending, dealing with, stockpiling, maintenance, and obliteration of biometric identifiers and data" (i.e., fingerprints, iris checks, voiceprints)[32]. It refuses private parties from collecting biometric identifiers and producing person "profile" data got from biometric identifiers without first telling the people whose data is being gathered, acquiring their assent, and making explicit revelations to them. The resolution additionally requires private gatherings to distribute definite data with regard to their information maintenance and annihilation approaches and forbids them from selling collected biometric identifiers.

[32]Michael Hintze, In Defense of the Long Privacy Statement, 76 MD. L. REV. 1044 (2017).

CHAPTER-5: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN INDIA.

5.1. Introduction

Biometric data security has the appearance of the way forward for the Indian government in its advantages towards identification. The Indian government uses the biometric data security system from their unique identification scheme also known as the Aadhaar scheme to election IDs. As a result, the law of privacy in India is increasingly being challenged by new technologies and practices. The new biometric technologies work with developing the collection and sharing of personal data. The Right to access to data held by government bodies (RTI) gives that people have a fundamental basic liberty to demand data held by government bodies[33]. Thus, in this chapter of this research paper needs to examine the Biometric data security and the right to privacy in India with the examination of the relevant rules and regulations.

5.2. Regulation of Biometric Data in India

The Information Technology Rules, 2011 in India, illustrate 'private data' as data that connects with a characteristic individual and can be utilized to distinguish that person, either alone or in blend with other accessible data[34] i.e., personal data[35]. In this case, the law in relation to privacy has a more significant level of safety and more tight standards for handling, managing, or dealing

[33]Boersma et al. [4] See pages 170–185. Available at SSRN: https://ssrn.com/abstract=2437990 (Access on-11.04.2022).
[34] Ibid.
[35] Personal data means facial scan, fingerprints, eye scan and so forth.

with any information or delegated Sensitive Data[36], which is clearly laid down in the Information and Technologies Act, 2000 (IT Act). However, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 also referred to as privacy rules clearly define personal information and sensitive personal data, including biometric data[37]. Besides, some other laws adopt certain uses of biometric data, such as authenticating an individual's identity through the Aadhaar card[38].

5.3. Biometric Data and Personal Data Protection Bill

Both the above-mentioned acts namely IT Act 2000 and Information Technology Rules 2011 are standard with the developing technologies concerning personal data protection in India. For this reason, the Indian government set up a specialist board in 2017, led by Justice B. N. Srikrishna for reform of the biometric data and personal data protection bill. The above-mentioned board had unstructured to submit their draft bill before the public authority named as "Personal Data Protection Bill"[39]. Subsequently, the said board submitted their draft bill before the parliament in the year of 2019. The Bill lays out India's information security system and is supposed to replace the ongoing structure[40]. Moreover, the Bill recommends that a duplicate of such information be kept up within an Indian server farm. Punishments have been proposed for disregarding regulations controlling biometric information handling or collecting, promoting, sending or selling biometric information intentionally, purposely, or foolishly[41].

[36]The most recent legislation to be made public is the Privacy Bill 2014, CIS India, April 3, 2014. Available at: http://www.medianama.com/2014/04/223-leaked-privacy-bill-2014-vs-2011-cis-india/ (Access on-11.04.2022).
[37] Ibid.
[38]Next Generation Identification officially replaces IAFIS, CJIS Link, Volume 16, Number 2, October 2014. Available at: https://www.fbi.gov/services/cjis/cjis-link/ngi-officially-replaces-iafis-yields-more-search-options-and-investigative-leads-and-increased-identification-accuracy See also: Next Generation Identification Page, Federal Bureau of Investigation. (Access on-11.04.2022).
[39] Ibid.
[40] Ibid.
[41]Bloomberg BNA Privacy & Security Law Report 1353 (2015);

5.4. Use of Biometric Data, Post Aadhaar[42] Period

At the stage of this study, it can be seen that the Supreme Court of India, in Justice *Puttaswamy (Retd.) and Anr. v Union of India and Ors*., maintained general legitimacy of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "Aadhaar Act")[43]. The brief facts of the case is that the Uttar Pradesh government conceptualised a scheme for the unique identification of the below poverty line families[44]. After that the retired Justice K.S. Puttaswamy filed a writ petition before the supreme court of India to challenge the policy of the government regarding the Aadhar card.[45] After hearing the matter, on 10.05.2018 the Supreme Court held that the design of the Aadhaar Act excludes the fundamental principle i.e., biometric data protection in relation to privacy[46]. Justice Chandrachud emphasized that acceptable rules have to be laid down for every step since the compilation to preservation of biometric data rely on the knowledgeable consent, along with identifying the time period for retention. The people have to be given the right to access, correct and delete data. An opt-out decision should be essentially offered in this case[47]. Hence, the Supreme Court of India agreeing with the Petitioners and found that the Aadhaar Act to be devoid, therefore, of all these safety- valves. And in doing so, the judge by extension pitched an argument against data-trafficking and data- brokerage echoed, for example, in the highly protective legal regime sought to be introduced through the Indian draft 'Personal Data Protection Bill, 2018'[48]. In India, they did not recognize the right to privacy law as fundamental rights, but after the pronouncement of Aadhaar[49] case, the Supreme

[42] Supra note-02.
[43] Justice K.S. Puttaswamy (Retd.) v. Union of India (Puttaswamy I), Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aug. 24, 2017).
[44] Ibid.
[45] Ibid
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Supra note-02

Court of India recognised the protection of biometric data in relation to right to privacy as fundamental right by amending Section 57 of the Aadhar Act 2016.

5.5. Conclusion

Accordingly, at the end of this chapter, it can be seen that biometric data would be considered as sensitive data under the principle laid down in privacy law. The present legal system of India reflects the protection of biometric data as sensitive data under the Privacy Rules, and the Aadhaar Act determines a specific use-case for biometric data security. Besides, the expected purposes and abuses of biometric data are incomprehensible. Therefore, the government of India needs strict rules for the security of biometric data and the law of privacy of an individual.

CHAPTER-6: BIOMETRIC DATA SECURITY AND THE RIGHT TO PRIVACY IN BANGLADESH.

6.1. Introduction.

In recent times in Bangladesh, biometric technology is widely used in the context of border security, voting system, health care system, education system, and so on. However, the said technology has a huge privacy concern in countries i.e., Bangladesh, because there are some insufficient legal frameworks for the protection of biometrics data security and right to privacy law[50].

6.2 Regulation of Protection of Biometric Data in Relation to Right to Privacy in Bangladesh

In Bangladesh, there are no clear provisions of law or statute in order for securing the Biometric data security and privacy law. In this case, the proviso laid down under Article- 43(b) of the Constitution of the People's Republic of Bangladesh provides that every citizen shall have the right to the privacy[51]. The government of Bangladesh for the first time in 2006 passed the Information and Communication Technology Act, 2006 for the security of data protection and the law of privacy[52]. Section 2 (20) of the said Act defines the term data including personal and

[50]R. E. O. Paderes, A Comparative Review of Biometric Security Systems, Proc. - 8th Int. Conf. Bio-Science Bio-Technology, BSBT 2015, 8–11, 2016.
[51] Article 43, Constitution of the people's Republic of Bangladesh, Available on- http://bdlaws.minlaw.gov.bd/act-details-367.html#:~:text=Members%20of%20Parliament%20shall%20be,order%20made%20by%20the%20President. Access on- 11.04.2022.
[52]Bangladesh Information Communication Technology Act, 2006, available at http://www.icnl.org/research/library/files/Bangladesh/comm2006.pdf. (Access on- 11.04.2022)

sensitive data and its protection[53]. Sections 54 and 57 of the ICT Act, 2006 also provide the security of the data as specified under Section 2 (10) of the said Act and the law of privacy of any person in digital form[54]. But the Act was hugely criticised by all quarters of the society. Thereafter, Sections 7 (h), 7 (i), and 7 (r) of the Right to Information Act, 2009[55] provide that any sort of personal information is protected by the law, and anybody cannot get any information regarding privacy or personal data"[56], but the term data is not specified in the said Act[57]. Furthermore, after the criticism and absurdity of the ICT Act, of 2006, Bangladesh passed the Digital Security Act 2018[58]. The Digital Securities Act, 2006 contains provision assurance of Identity Information.[59]" In this case, Section 26 of the Act defines "crimes relating to collecting and using identity information"[60]. The objective of the said Act is to prevent cybercrime and ensuring the digital security and safety of the law of privacy in Bangladesh.

6.3. Data Protection Authority

In Bangladesh, the data protection guidance and formulation are generated by the National Data Security Centre and the executive matters i.e., blocking content or decrypting a data source are controlled by Digital Security Agency (DSA) under the Digital Securities Act, 2018[61]. In this case, it can be seen from the wording of the Digital Security Act 2018 that "if any person without any

[53] Ibid.
[54]Ibid.
[55]Section 7 (h), 7 (i) and 7 (r) of the Right to Information Act, 2009, Available on- https://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/bangladesh/bangladesh_rti_act_2009_summary.pdf Access on- 11.04.2022.
[56] Ibid.
[57] Ibid.
[58]Bangladesh Digital Security Act, 2018, available at https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf.
[59] Digital Securities Act, 2018- Available at- https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951#:~:text=These%20cases%20have%20one%20thing,of%20expression%2C%20especially%20in%20cyberspace. Access on 12.04.2022.
[60] Ibid.
[61]*S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell, Privacy, security, and surveillance in the global south: A study of biometric mobile SIM registration in Bangladesh, Conf. Hum. Factors Comput. Syst. - Proc., (2017) 906–918.*

legal authority collects, sells, takes possession, supplies, or uses any person's identity information, then that activity will be an offense under the Act"[62].

6.4. Conclusion

Accordingly, the concept of biometric data privacy and fundamental data protection privileges and necessities is latest in Bangladesh, however, one that has never been as significant as in this period of quick digital progress, social networking, cybercrime, electronic correspondence, and expanding attention to clients/buyers.

[62]Ibid.

CHAPTER-7: COMPARATIVE ANALYSIS OF PROTECTION OF BIOMETRIC DATA IN UK, USA, INDIA AND BANGLADESH.

7.1. Introduction

There are no common legal provision or convention in the world are specific to biometric data protection. For this reason, the countries in the world rely on their own or domestic legislation in relation to personal data protection and right to privacy on board sense. But, such sort of legislation sometimes proves to be poorly adapted to biometric data protection concerning right to privacy. The legislation concerning biometric data protection and right to privacy in highly developed countries i.e., UK, USA and developing countries i.e., India and Bangladesh are not same. The main differences between the countries are their legal framework or legal system. This chapter will reveal the comparative analysis of biometric data security or protection in relation to right to privacy in UK, USA, India and Bangladesh based on their legal framework or system.

7.2. Comparative analysis of Protection of Biometric Data in Relation to right to privacy in UK, USA, India and Bangladesh.

This chapter of this research paper requires a discussion based on the comparative studies of data protection and the law in relation to right to privacy. In this case, it seems that biometric data security and the right to privacy are well secured by the UK[63]. This is because, in UK after incorporating the GDPR into their national legislation by the Data Protection Act, 2018, individual

[63]Ibid

privacy law and data protection are well settled[64]. Hence, the UK resolves the issue in GDPR and presents a complete arrangement to handle this calamity[65].

In comparison to data protection and the right to privacy law in UK, there is no complete, single and suitable government regulation in the USA regarding the guideline for handling and utilization of biometric information[66]. However, in BIPA and the Texas State of USA, there remain regulations over biometric data protection. Washington also passed a regulation on biometric information in June 2017[67]. Obviously, US controllers are likewise progressively zeroing in on the utilization of biometric information.

In contrast with UK and USA, the biometric data protection law and right to privacy law in India are not well protected. However, in India in a milestone case named Justice *K.S. Puttaswamy v Union of India*, the Supreme Court of India named biometric data security in relation to right to privacy as a 'fundamental right'[68]. Supreme Court of India additionally reached out by saying that biometric information insurance is currently on the top plan of the officials also[69].

On the other hand, Bangladesh has no privacy and data protection regulation till to date. On account of the utilization of biometric technologies, there is no obligatory approach or guidelines from Bangladesh Telecommunication Regulatory Commission (BTRC)[70]. Similarly, Bangladesh

[64] Ibid.
[65] Ibid.
[66]Ibid
[67] Ibid.
[68]KS Puttaswamy v. Union of India, (2017) 10 SCC 641
[69]Ibid.
[70]"Internet Subscribers in Bangladesh December, 2018. | BTRC." [Online]. Available: http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-december-2018. [Accessed: 03.05.2022].

passed Digital Securities Act, 2018 for biometric data protection, but there are no specific provisions regarding the protection of biometric data in relation to right to privacy[71].

Consequently, from the above comparative discussion regarding biometric data and the right to privacy between the UK, USA, India, and Bangladesh, it can be seen that Bangladesh does not have any data protection and the right to privacy laws like the UK, and the USA[72].

7.3. Conclusion

There is no express biometric data protection in relation to right to privacy law in developing countries i.e., Bangladesh and India. But Bangladesh and India can follow the higher developed countries i.e., UK GDPR system of biometric data protection law or USA BIPA system of biometric data protection law. This extraordinary protection strategy from the higher developed countries can be taken as an example in Bangladesh and India. Consequently, the citizens of Bangladesh and India can be given a lot of control over their personal data information and they can protect their right to privacy as well.

[71] Ibid.
[72] Ibid.

CHAPTER 8: CONCLUSION AND RECOMMENDATION

8.1 CONCLUSION

In analyzing biometric data protection in relation to right to privacy law in UK, USA, India and Bangladesh, it seems a reflection of their legal framework. Right to privacy, as protected in Article 12 of the Universal Declaration of Human Rights (UDHR)[73] where the charter explained that everyone has the right to privacy, which includes the important aspect that everyone has the right to protection of personal data concerning him or her, and such right extends to the right to protection of personal data on the web or internet. After given the primary tools of the law of data protection in relation to right to privacy and after discussing the comparative analysis of data protection in relation to right to privacy in UK, USA, India and Bangladesh as above identified, it appears that the UK GDPR considered a most influential instrument in terms of adoption and observance. This is because, UK-GDPR defines personal data and also provided the right to privacy and protection of personal data are, therefore, recognized as constituting fundamental rights. However, the USA after passing the BIPA, it seems that the USA has a well-established legal framework concerning biometric data protection in relation to privacy law. Moreover, in India, they have not well-established biometric data protection in relation to privacy law, but after the judgment of Aadhar card, the supreme court of India recognised the privacy law as a fundamental right, which also preserved the biometric data protection of an individual. A cautionary note is, however deserved here. Realistically, Bangladesh unlike UK, USA and India find themselves in a profound crossroads. This is because, Bangladesh has not any biometric data

[73] Article 12, Universal Declaration of Human Rights (UDHR)

protection in relation to privacy law. Though, Bangladesh constitution guaranteed the law of privacy under Article 43, but, they have not well-establish biometric data protection in relation to privacy law, mostly, they rely on the DSA 2018, but there is a notable absence in the abovementioned Act of any legislative demarcation between the concepts of 'security' and 'protection' and, resultantly, the substantive elaboration of the nature and ambit of data protection.

8.2 RECOMMENDATION.

This research paper establishes that there in Bangladesh there is no specific legislation regarding biometric data protection in relation to privacy. As a result, the legislative body of Bangladesh should be concerned with the biometric protection in relation to privacy. This is because, Bangladesh already entered into the digital era by implementing our current government election manifesto in 2009 election. So, our nation needs a new legislation concerning biometric data protection in relation to privacy law. Our culture has no concept of biometric data protection in relation to privacy law, for this reason, it needs to raise awareness about using biometric data fairly and securely. Another idea is that Bangladesh can rely on the UK-GDPR style data protection law. This is because, Bangladesh and UK legal system rely on common law legal system and Bangladesh judges in courts can use the UK GDPR by their persuasive powers. However, Bangladesh should make a framework for the “National Cyber Security Strategy”. This is because the current government is promised to make a digital Bangladesh and they are trying their best to digitalize the country since 2009. As a result, our current government set up a central database for the protection of the National Identification (NID) information and fingerprints of the citizens of our country. But, due to the imbalanced political environment and lack of specialists in this area, Bangladesh should set up a proper framework for the “National Cyber Security Strategy”.

BIBLIOGRAPHY

1. Primary sources:

a) STATUTES.

I. *Biometric Information Privacy Act (BIPA)*

II. *Data protection Act 2018*

III. *Information and Communication Technology Act, 2006 (ICT ACT)*

IV. *Information and Technologies Act, 2000 (IT Act).*

V. *Resolution 2322 (2016)*

VI. *The Aadhaar Act 2016*

VII. *The data protection Act, 1984*

VIII. *The Digital Securities Act, 2006*

IX. *The Digital Security Act 2018*

X. *The Security Council Resolution 2160 (2014)*

b) Cases:

I. *Justice K.S Puttaswamy (Retd.) and Anr. v Union of India and Ors.,*

II. *Justice K.S. Puttaswamy (Retd.) v. Union of India (Puttaswamy I),*

III. *Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019)*

IV. *Lloyed v Google LLC [2021] UKSC 50.*

2. ***Secondary source:***

a) ***Books and Journalsl:***

i) *Brad Smith, Carol Ann Browne "Tools and Weapons: The Promise and the Peril of the Digital Age", 2019: Hodder & Stoughton*

ii) *David Baniser, "The Right to Information and Privacy: Balancing Rights and Managing Conflicts", 2011: World Bank Institute).*

iii) *"NY State Senate Bill S1933. NY State Senate. 2021-01-16. Accessed on 10.04.2022.*

iv) *Fisher, Sandra L. (2020). University of Twente Research Information System (RIS).*

v) *Bloomberg BNA Privacy & Security Law Report 1353 (2015);*

vi) *L. Amoore, "Biometric borders: Governing mobilities in the war on terror," Political geography, Vol. 25, No. 3, pp. 336-351, 2006.*

vii) *Michael Hintze, In Defense of the Long Privacy Statement, 76 MD. L. REV. 1044 (2017).*

viii) *Michael Hintze, In Defense of the Long Privacy Statement, 76 MD. L. REV. 1044 (2017).*

ix) *R. E. O. Paderes, A Comparative Review of Biometric Security Systems, Proc.- 8th Int. Conf. Bio-Science Bio-Technology, BSBT 2015, 8–11, 2016.*

x) *R. E. O. Paderes, A Comparative Review of Biometric Security Systems, Proc. - 8th Int. Conf. Bio-Science Bio-Technology, BSBT 2015, 8–11, 2016.*

xi) *S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell, Privacy, security, and surveillance in the global south: A study of biometric mobile SIM registration in Bangladesh, Conf. Hum. Factors Comput. Syst. - Proc., (2017) 906–918.*

xii) *[1]Security Council, Security Council Resolution 2160, S/RES/2160 (United Nations 2014), para. 18.*

xiii) *Security Council, Security Council resolution 2322, S/RES/2322 (United Nations 2016), para 3.*

xiv) *Kidd, S. 2011. Good practice in the development of management information systems for social protection. Pension watch Briefings on social protection in older age. Briefing no.5 (helpage International, London).*

xv) *Dijkhoff, T.; letlhokwampedi, G. (eds.). 2017. Recommendation on Social Protection Floors: Basic Principles for Innovative Solutions (The Netherlands, Kluwer Law International B.V.).*

xvi) *5 Victoria A. Espinel, Cybersecurity threats defy national borders, so countries should collaborate, not clam up, South China Morning Post.*

b) <u>Online sources:</u>

I. *US v Jones, 615 F. 3d 544, available at-https://www.law.cornell.edu/supremecourt/text/10-1259 (Access 27. Mar.2022).*

II. *"Right of privacy." Merriam-Webster.com Legal Dictionary, Merriam-Webster, https://www.merriam-webster.com/legal/right%20of%20privacy. (Accessed 27 Mar. 2022).*

III. *Boersma et al. [4] See pages 170–185. Available at SSRN: https://ssrn.com/abstract=2437990 (Access on-11.04.2022).*

IV. *Future of Privacy Forum, "Mobile location analytics code of conduct," 2013 [Online]. Available: http://www.futureofprivacy.org/wp-content/uploads/10.22.13- FINAL-MLA-Code.pdf. (Acess on 02.05.2022).*

V. *Next Generation Identification officially replaces IAFIS, CJIS Link, Volume 16, Number 2, October 2014. Available at: https://www.fbi.gov/services/cjis/cjis-link/ngi-officially-replaces-iafis-yields-more-search-options-and-investigative-leads-and-increased-identification-accuracy See also: Next Generation Identification Page, Federal Bureau of Investigation. (Access on-11.04.2022).*

VI. *The most recent legislation to be made public is the Privacy Bill 2014, CIS India, April 3, 2014. Available at: http://www.medianama.com/2014/04/223-leaked-privacy-bill-2014-vs-2011-cis-india/ (Access on-11.04.2022).*

VII. *'The Right to Privacy' (Lawteacher.net, April 2022) <https://www.lawteacher.net/free-law-essays/human-rights/right-to-privacy.php?Vref=1> accessed 19 April 2022*

VIII. *Troy Hunt: The 773 million Record 'Collection #1' Data Breach. [Online]. Available: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/. [Accessed: 26-Mar.-2022]*

IX. *U.S. Department of Health, Education and Welfare (HEW), Records, Computers, and the Rights of Citizens (1973), at 41, https://www.justice.gov/opcl/docs/rec-com-rights.pdf; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), http://www.oecd.org/internet/ieconomy/oecd*

guidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm); U.S. Federal Trade Commission (FTC), Privacy Online: A Report to Congress (1998), at 7, https://www.ftc.gov/sites/default/files/ documents/reports/privacy-online-report-congress/priv-23a.pdf); Asia-Pacific Economic Cooperation (APEC), Privacy Framework (2005), https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-privacyframework/05_ecsg_privacyframewk.pdf). Access on-08.04.2022.

X. *Centre for Information Policy Leadership. 2014. A Risk-based approach to privacy: Improving effectiveness in practice. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1- a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf. [Access on -05.05.2022].*

XI. *Chirchir, R.; Farooq, S. 2016. Single Registries and Social Registries: clarifying the terminological confusion, Pathways' Perspectives on social policy in international development, Issue No. 23, November 2016 Kent, United Kingdom, Development Pathways). Available at: http://www.developmentpathways.co.uk/resources/wpcontent/uploads/2016/11/Single-and-Social-Registries.pdf [05.05.2022].*

XII. *Simon Kemp, digital in 2018: World's internet users pass the 4 billion mark, available at https://wearesocial.com/blog/2018/01/global-digital-report-2018.*

XIII. *2 anmarfrangoul, 10 ways the web and internet have transformed our lives, CNBC, available at https://www.cnbc.com/2018/02/09/10-ways-the-web-and-internet-have-transformed-our-lives.html.*

XIV. *3 Victoria A. Espinel, Cybersecurity threats defy national borders, so countries should collaborate, not clam up, South China Morning Post, available at https://www.scmp.com/comment/insight-opinion/article/2144126/cybersecurity-threats-defy-national-borders-so-countries.*

XV. *4 Centre for Long Term Cybersecurity, Asian Cybersecurity Features, available at https://cltc.berkeley.edu/wp-content/uploads/2017/12/asianfutures.pdf.*

XVI. *6 Security Magazine, Which Countries Have the Worst and Best Cybersecurity? Available at https://www.securitymagazine.com/articles/89829-which-countries-have-the-worst-and-best-cybersecurity.*

XVII. *7 Roartech, Can Sri Lanka's Cyber Security Strategy Protect Us? Available at https://roar.media/english/tech/insights/can-sri-lanka-s-cyber-security-strategy-protect-us/.*

XVIII. *8 Kathmandu Post, 19 govt sites breached in latest cyberattack, available at https://kathmandupost.com/valley/2017/11/04/19-govt-sites-breached-in-latest-cyberattack*