

DIGITAL FOOTPRINTS: A RIGHTS-BASED PERSPECTIVE

AUTHORED BY
JUSTICE DR. SYED REFAAT AHMED
HONOURABLE JUDGE
SUPREME COURT OF BANGLADESH





Justice Dr. Syed Refaat Ahmed (Justice Ahmed) was born on 28 December 1958 in London, United Kingdom. His parents are Late Barrister Syed Ishtiaq Ahmed and Late National Professor Dr. Sufia Ahmed. He obtained his LL.B (Hons) degree from the University of Dhaka and secured First Class, First position. Justice Ahmed did his B.A. and M.A. from Wadham College, University of Oxford. He did his M.A. in Law and Diplomacy and Ph.D. from The Fletcher School of Law and Diplomacy, Tufts University. He was Ford Foundation Fellow in Public International Law at the Fletcher School.

Justice Ahmed has previously worked as a lawyer in the City of London and with the United Nations High Commissioner for Refugees in Hong Kong and Washington, D.C., and prior to his elevation as an Additional Judge of the High Court Division, Justice Ahmed was a Partner at Syed Ishtiaq Ahmed & Associates (SIA&A), Law Consultants and Practitioners, Dhaka, Bangladesh. At SIA&A, Justice Ahmed accomplished extensive Chamber and Court practice in the fields of constitutional, commercial, company, and fiscal law; including other areas of expertise in joint-venture enterprises, civil engineering construction, fertilizer industry, gas and oil exploration, telecommunication, intellectual property (copyright, trademark) information technology, and immigration law. He successfully represented clients before the World Bank Administrative Tribunal in a sexual harassment case and in arbitration conducted under the Rules of Conciliation and Arbitration of the International Court of Arbitration of the International Chamber of Commerce.

He was elevated as Additional Judge of the High Court Division on 27 April 2003 and appointed Judge of the same Division on 27 April 2005. Justice Ahmed has adjudged an extensive range of cases, of which the more significant Judgments are in the fields of constitutional Law, civil revision, admiralty, arbitration, company, labour/Employment and Trade Mark Laws, Customs and VAT Laws, Death Sentence Confirmation References along with Criminal Appeals that have appeared regularly since 2005 in mainstream law reports in Bangladesh, notably the Dhaka Law Reports (DLR), Bangladesh Legal Decisions (BLD), Bangladesh Law Chronicles (BLC), Law Guardian (LG), Bangladesh Law Times (BLT), The Law Reporter (TLR), The Apex Law Reports (ALR), The Counsel Law Reports (CLR) and the Legal Circle Law Reports (LCLR).

Amongst the myriad of cases adjudged by Justice Ahmed the most notable ones include the Judgments delivered in Mohammad Badiuzzaman vs. Bangladesh and Others, A.B.M. Khaliqzaman and Others vs. United Commercial Bank and Others, Axiata (Bangladesh) Ltd. alias Robi Axiata Ltd. vs. Govt. of Bangladesh & others, Md. Mehdi Hassan and Another vs. The Government of Bangladesh and Others, and Moulana Md. Abdul Hakim v. Govt. of Bangladesh & Ors.

In *Mohammad Badiuzzaman vs. Bangladesh and Others* [7LG (2010) HCD, 208 and 15BLC (2010) 531] the Court dealt with a constitutional challenge to the execution of the Chittagong Hill Tracts (CHT) Peace Accord of 1997 and found the Peace Accord to be a political accord between belligerents and, thereby, not to be a subject of Judicial Review, and the concomitant and corresponding challenge to the CHT Regional Council Act, 1998 stemming from the execution of the CHT Peace Accord, was found to be a colorable piece of legislation given that the establishment of the Regional Council and its consequential powers envisaged in the Act were uncovered to be potentially destructive of the fabric of a unitary Republic.

In *A.B.M. Khaliquzzaman and Others vs. United Commercial Bank and Others* [28 BLD (HCD) 2008, 635] otherwise known as the UCBL Case, a case considered as the first of its kind under the Companies Act, 1994 read with the Depository Act, 1999 and the Depository (User) Regulations, 2003, ensured the protection of the interests of small-time shareholders against machinations of major equity investors to defeat the interests of the former group's dividend entitlements by resort to a pre-fixed Record Date as determinant of closure of the company's Share Register.

In the notable *Axiata (Bangladesh) Ltd. alias Robi Axiata Ltd. vs. Govt. of Bangladesh & others* [1 LCLR (2012) HCD 77] judgment the Court dealt with a revenue matter of some significance. It was held that in granting or renewing Cellular Mobile Phone Operator's Licenses, assignments of spectrum etc., the Bangladesh Telecommunication Regulatory Commission (BTRC) acts as a statutory body that provides statutory taxable service under the Bangladesh Telecommunication Act, 2001 read with the Value Added Tax Act, 1991, hence BTRC, as the regulator for telecommunication sector, exercises statutory power and engages in taxable economic activity, and therefore it is incumbent on a licensee of the BTRC, as a recipient of taxable services supplied by BTRC, to deduct or withhold VAT at source after calculating the same on the entire consideration and thereafter pay directly into the exchequer as the deducting party.

In the judgment in *Md. Mehdi Hassan and Another vs. The Government of Bangladesh and Others* [1 LCLR (2012) HCD 380] which has emerged as a landmark ruling both with regard to issues of maintainability and enunciation of definition of 'worker' under the Labour Act, 2006. The Court found that the Board of Trustees of Unilever's Workers Participation and Welfare Fund exercises its powers under the Labour Act, 2006, and thus it performs public/governmental functions, hence the illegalities of the Board are amenable to the writ jurisdiction, and furthermore set the standards for determining whether an employee is a worker or not include such employee having certain powers specified by the Court.

In the ruling in *Moulana Md. Abdul Hakim v. Govt. of Bangladesh & Ors.* [34 BLD (HCD) 2014, 129] the Court explored the judicial reviewability of actions and decisions of private bodies operating in the public domain. This judgment, questioned the conventional wisdom, identified amenability to judicial review not exclusively by reference to an obvious derivative public status of a person but increasingly by the public domain within which it operates and prevails irrespective of its derivative status, and that a Writ in Certiorari under Article 102(2) can only validly be addressed to public functionaries was found as fallacious as it belies the fact of public functionaries forsaking their monopoly over public affairs and of private and public enterprise being inextricably intertwined in the conduct of business of the Republic or of a local authority.

These aside, Justice Ahmed has delivered Judgments in numerous Public Interest Litigations (PILs) and Criminal Miscellaneous cases, that have also appeared in journals or are to be found reported in websites/online case law databases as Chancery Law Chronicles and at www.thinklegalbangladesh.com. Two significant PIL Judgments authored by Justice Ahmed in *Syed Saifuddin Kamal vs. Bangladesh, Ministry of Health* [38 BLD (2018), 453], and in *Human Rights and Peace for Bangladesh vs. Bangladesh* (Writ Petition No. 14258 of 2012), addressed the tradition of correcting a wrong or filling legal and administrative lacunae requiring multi-dimensional strategies, and epitomize the cooperative or collaborative efforts on the part of the petitioner, State or public authority and the Court to secure the observance of constitutional or legal rights and vindicate public interest. In *Syed Saifuddin Kamal vs. Bangladesh, Ministry of Health*, the Court through a collaborative exercise spurred

and guided the formulation of the “Emergency Medical Services for Road Accident Victims and Protection of Good Samaritans Policy, 2018”, and similarly, in *Human Rights and Peace for Bangladesh vs. Bangladesh* (Writ Petition No. 14258 of 2012) the Bangladesh Telecommunication Regulatory Commission, under the Court’s guidance, formulated the “Guidelines for Limiting Exposure to Radiation of Electromagnetic Fields (9 Khz to 300 Ghz)”.

Justice Ahmed has the honour of being frequently invited as the Chair, Chief Guest and Keynote Speaker at various forums including adjudging Moot Court Competitions and has a number of publications and lectures to his credit extensively at home and abroad on varied aspects of the law, especially on international migration and refugee law, constitutional law and the environment and climate change. Cited below are a few of the publications authored and lectures delivered by Justice Ahmed encompassing varied subjects and disciplines:

- Aspirational Value of Law: Test Case on Workers’ Rights (Delivered as the Justice Muhammad Ibrahim Memorial Lecture, 2018 at the Asiatic Society of Bangladesh, Dhaka on 13 October, 2018) 2019 (4) Legal Issue, 42;
- Constitutional Law and Peace Accords: the case of the Chittagong Hill Tracts (Delivered as the Sarat Chandra Bose 125th Birth Anniversary Lecture, 2014 in Kolkata, India on 12 July, 2014) 2018 (1) Lawyers and Jurists (LNJ), Journal-1;

- Beyond The Maze: Streamlining Labour Recruitment Process in Bangladesh, ed. Tasneem Siddiqui, Dhaka: Refugee and Migratory Movements Research Unit, February 2002, 58-60; presented at the National Workshop on Streamlining Labour Recruitment Process of Overseas Employment, 24 September, 2001;

- Persecution: The Vietnamese Paradigm, Journal of The Asiatic Society of Bangladesh, Humanities, Volume 46, No.2, December 2001, 373-386;

- Forlorn Migrants: An International Legal Regime for Undocumented Migrant Workers, Dhaka: The University Press Limited, 2000;

- Fifty Years of Universal Declaration of Human Rights-An Overview: Proceedings of the British-Bangla Law Week, 29 November-5 December 1998, presented at the British- Bangla Law Week, Session on Refugees and Migration, The British Council, Dhaka; and

- The Role of the UN Secretary-General in Resolving the Iran-Iraq Conflict, 1982-1987: Establishing a Case for an Effective Peace-Making Process, Bangladesh Institute of International and Strategic Studies Journal, Volume 11, No.2. April 1990, 208-241.

- “The Rohingya Asylum Dilemma: Setting Sights Beyond Protection”, delivered at the Professor Mahfuza Khanam and Barrister Shafique Ahmed Trust Fund Lecture 2019, under the auspices of the Asiatic Society, on 9 July, 2019;

- “Politics of Conflicting Allegiances: Bengal, 1937-40”, delivered at the Professor Dr. Habiba Khatun Trust Fund Lecture 2019, under the auspices of the Department of Islamic History and Culture, University of Dhaka, on 16 April, 2019;

- “Deconstructing Judicial Independence”, Inaugural Lecture delivered at the Think Legal Lecture Series, at the Edward M. Kennedy (EMK) Center for Public Service and the Arts on 10 January 2015.

Justice Ahmed’s passion for authoring also comprises of the editing of two books, authored by Late Barrister Syed Ishtiaq Ahmed – the most sought after and celebrated luminary in the history of the legal field in Bangladesh, entitled The Ishtiaq Papers, published by The University Press Limited in 2008, and the Certiorari: An Administrative Law Remedy, published by Mullick Brothers in 2011.

In 2016 he played an instrumental role in organizing the South Asia Judicial Conference On Environment And Climate Change held under the joint auspices of the Supreme Court of Bangladesh, the Asian Development Bank and the Asian Judges Network on Environment, held in Dhaka from 25-26 November, 2016. Justice Ahmed has been associated variously in a teaching/advisory/consultative capacity with esteemed institutions like the Bangladesh Bar Council’s Legal Education and Training Institute (LETI), Refugee and Migratory Movements Research Unit (RMMRU) of the University of Dhaka, National Defense College (NDC), Police Staff College, National University, Ain O Salish Kendra (ASK), Welfare Association of Repatriated Bangladeshi Employees (WARBE), various Non-governmental Organizations etc.

Justice Ahmed's affiliations, with innumerable national and global bodies is evident in the fact that he is a Founder Member of the Global Judicial Institute for the Environment, Brazil; Life Member of the Asiatic Society of Bangladesh; Former Acting Chairman to The Bangladesh Judicial Service Commission; Member, Advisory Committee to the Joint Project of the Ministry of Home Affairs, Government of Bangladesh and German Technical Cooperation-GTZ, "Improvement of the Real Situation of Overcrowding in Prisons in Bangladesh"; The Oxford Union Society; Bangladesh Institute of Law and International Affairs; South Asians for Human Rights; The British Alumni Association in Bangladesh; The Fletcher Alumni Group; and Member to the Supreme Court Judicial Reforms Committee, Bangladesh.

Justice Ahmed, in addition of being an eminent persona in the legal fraternity in Bangladesh, is an "Aficionado Collector" since the late 1960s of film, music and theatre memorabilia, recordings, magazines, books, pamphlets, filmographies etc., a Curator of a private archive-exhibit 'ARCHIVA' dedicated to the objects antiquated in their representation and outmoded in their format, and an intrepid traveler who has travelled and explored exotic places like Brazil, U.S.A., U.K., Ireland, The Netherlands, France, Monaco, Spain, Portugal, Germany, Switzerland, Italy, The Vatican City State, Greece, Turkey, Bahrain, Qatar, U.A.E., Pakistan, India, Nepal, Sri Lanka, Myanmar, Thailand, Cambodia, Malaysia, Singapore, Macau, Hong Kong, and The Philippines.

PROLOGUE

Epochs of sustained innovations and the industrial enterprise they spur are typically characterized as 'revolutions'. This is because these periods are marked by unprecedented systemic upheavals reordering human enterprise and interactions. The law intervenes in this context to regulate such activity by innovation, ingenuity and adaptability.

At the brink of a Fourth 'Digital'/Industrial Revolution spurred by the previous epoch's technological advancements, the 'human factor' both driving and driven by such changes gains prominence.

As noted by Klaus Schwab, Founder and Executive Chairman, World Economic Forum in *"The Fourth Industrial Revolution: What it means, how to respond"* (2016), the Fourth Industrial Revolution (4ir) is *"characterized by a fusion of technologies that is blurring the lines between the biological, physical and digital spheres."* On the matter of the overall impact on people, Schwab opines that the *"Fourth Industrial Revolution will change not only what we do but also who we are. It will affect our identity and all the issues associated with it: our sense of privacy, our notions of ownership, the time we devote to work and leisure and how we develop our careers, cultivate our skills, meet people, and nurture relationships"*.

In a similar vein the World Economic Forum in its “*Global Risks Report 2020: Insight Report - 15th Edition*” notes that the “*The Fourth Industrial Revolution (4ir)* has created an environment in which disruptive technologies and trends such as *Internet of Things (IoT)*, robotics, virtual reality (VR) and artificial intelligence (AI) are changing the way we live and work”. The question to be posed is whether time is now ripe for us to take control and charge of our parallel digital lives, being alter egos to our individual biological existence, in the context of the emergence of a new generation of rights? My answer is in the affirmative.

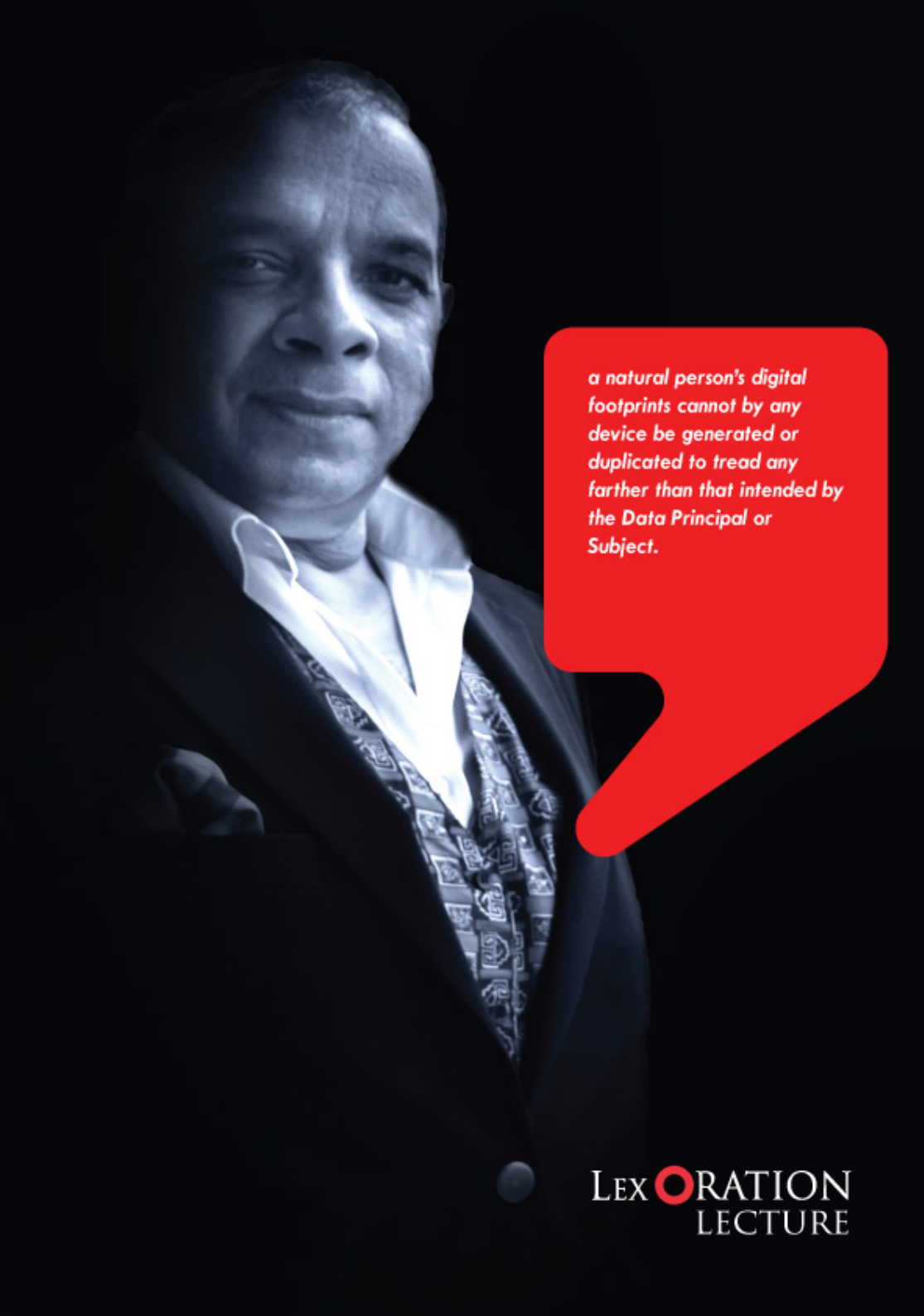
EMERGING NEED FOR DATA PROTECTION

Regulations/Legislations

Data are considered as the new oil in the age of the 4ir. Everyday a huge amount of data is being created and stored and it continues to grow at an unprecedented rate.

Due to the enormous use of technology, be it surfing on websites or using e-commerce platforms for trading or business, or use of social media, vast amount of **personal data or digital footprints** are being created, shared and transferred around the globe instantaneously, which in general results in personal data being irregularly and carelessly processed, thereby, posing a challenge for citizens/individuals to maintain control of their personal information.

Data protection regulations/ legislations provide the means to safeguard and protect **personal data**, as well as ensure that individuals have **autonomy of control of their personal data**, and are able to seek legal recourse or judicial intervention if such privilege is jeopardized or adversely affected, and ensuring to them the discretion whether or not they wish to share their information, determine who can have access to it, for how long, for what reason, and so forth. The emergence of an overarching right to privacy shielding our personal digital life arises here, accordingly.



a natural person's digital footprints cannot by any device be generated or duplicated to tread any farther than that intended by the Data Principal or Subject.

INTRODUCTION

Brad Smith's example below offers a simile or metaphor the significance of which should not be lost on us.

"You seal an envelope and give it to an agency of the government itself ... and the government cannot open an envelope and look inside without a search warrant based on probable cause, even though the government's postal service is in possession of that envelope.

People have a right to privacy on their sealed letters."

RIGHT TO PRIVACY AND RIGHT TO DATA PROTECTION

Right to privacy, as enshrined in article 12 of the Universal Declaration of Human Rights (UDHR) that

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”

means 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.

The European Union Data Protection Directive (Directive 95/46/EC, sec. 2[a]), considered a most influential instrument in terms of adoption and adherence, defines Personal Data “as any information relating to an identified or identifiable natural person (‘Data Subject’) and “an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”

Right to privacy and protection of personal data are, therefore, recognized as constituting fundamental rights. According to the *Charter of Human Rights and Principles for Internet* adopted by the Internet Rights and Principles Coalition (IRPC) under the auspices of the United Nations Internet Governance Forum, right to privacy is predicated on protection of the virtual personality, freedom from surveillance and freedom from defamation, etc.; and right to protection of personal information includes, amongst others, protection of personal data, obligation of data collectors, minimum standards on use of personal data, etc.

**DATA PROTECTION AS
A COMPOSITE CONCEPT
DEALING WITH PROCEDURAL
SAFEGUARDS**

**RIGHT TO PRIVACY BROKEN DOWN
(WITH RTI AND HABEAS DATA)
- THE EMERGENCE OF FOURTH
GENERATION RIGHTS?**

A rights-based approach unavoidably centres around the issue of data protection. Data protection deals with personal data and is grounded on certain fundamental principles such as, personal data–

- shall be processed fairly and lawfully;
- shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with the purpose they were consented/authorized for;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- shall be accurate and, where necessary, kept up to date;
- processed for whatever purpose/s shall not be kept for longer than it is necessary for that purpose/s;
- must be handled by legal/authorized persons.

Right to privacy allows an individual a fundamental right to control the collection of, access to, and use of personal information about them that is held by governments or private entities. On the other hand, right to information (RTI) bestows a fundamental right to any individual to access information held by government or public bodies. These two facets of the law are often portrayed as *“two sides of the same coin”*, and both rights being human rights, neither privacy nor access to information takes precedence over the other. Privacy can in this context be also portrayed and understood as individual autonomy encompassing the *“right to be left alone”*.

It is to be noted that every RTI legislation has an exemption for personal privacy. Deduced from a comparative study of different models of legislation (i.e., either combined or individual legislations covering both subjects) and policy making is that both RTI and data protection laws must clearly define how personal information is going to be considered and set out clearly the boundaries on types of personal information to be protected. Both aspects demand further a balancing test between personal harm and serving of public interest. (See, David Baniser, “The Right to Information and Privacy: Balancing Rights and Managing Conflicts”, 2011: World Bank Institute)

In many jurisdictions, the two rights are intertwined constitutionally under the concept of “Habeas Data” (which in Latin means “you should have the data”) i.e., a constitutional right that permits individuals to demand access to their own

information and to control its use. (See, Guadamuz (2001); and the Rule on the Writ of Habeas Data, issued by the Philippines Supreme Court (A. M. No. 08-1-16-SC, January 22, 2008). Accordingly,

“The action of Habeas Data, or the right to obtain personal information contained in public or private databases, has been very important in many countries in exacting accountability for human rights abuses and helping countries scarred by human rights abuses reconcile and move forward.” (See, Canton’s remarks of October 30, 2002).

In breaking down the general overarching right to privacy, one is confronted with new formulations of interests and rights operative within a specific digital sphere which I would like to term and identify as **Fourth-Generation Human Rights.**

Broadly enumerated, these rights encapsulate

1. The right to have personal data minimized- Companies should challenge themselves to strip identifying information from consumer data or avoid collecting it in the first place.
2. The right to knowledge- We should know what data is being collected and why.
3. The right to access- Companies should make it easy to access, correct and delete my own personal data.
4. The right to data security- The right to data security, without which trust is impossible.

Those of us familiar with the *ratio decidendi* and directions given in the *People’s Union of Civil Liberties (PUCL) vs. Union of India & Ors.* (reported in *AIR 1997 SC 568*) guarding against indiscriminate telephone-tapping and interception of messages ostensibly in the interest of public safety for emergency may pause to reflect on how prescient the court had been in providing content to these rights we now speak of.

Corollary to the issue of such rights is that of a regulatory régime overseeing the collection, usage, transfer and disclosure of personal data. Complex schemes have sprouted up in various jurisdictions striking a balance between the protection of fundamental rights

and freedoms and necessary, but proportionate, restrictions requisite for democratic governance and safeguarding national and public security. Resultantly, a host of rights pertaining to information collection, access, rectification, erasure, restricted processing etc. have all come to be defined by corresponding limiting provisions.

All this plays out against a primarily tripartite regulated relationship (reflected in what I would term as a “Data Trinity”) between (a) the *Data Principal* or *Data Subject*, i.e., natural person to whom the personal data relate to or, in other words, the individual creating the digital footprints, (b) the *Data Fiduciary* or *Data Controller*, i.e., the State,

natural or legal persons who on their own or collectively control and determine the purpose and means of processing such personal data, and (c) the *Data Processor*, i.e., those, including the State, who actually process such data on behalf of such controlling and determining authority. Such roles assumed are at their core, and regardless of the terminology used to define them, predicated on the fundamental concept of trust reposed by a natural person in the entire system evident in the collection, storage, access and dissemination of information about the **digital footprints** of such a person to whom personal data relate. It follows that the régime overseeing the entire enterprise of collection, storage, processing and dissemination, from a **rights-based perspective**, is intended to be beneficial to the Data Principal or Subject. The notions of privacy protection and consent are fundamental to the functioning of such a régime. The **data footprints** I speak of, of course, remain individual to such *Data Principal* or *Subject* and fall within the realm of personal privacy of such individual. Accordingly, any collection, use, processing into and dissemination of information, transfer etc. of such private details necessarily requires the consent of the *Data Principal* or *Subject*. In other words, the concept

of *data handling and use* in such a regulatory régime meets its limits in the requirement of consent.

The *EU General Data Protection Regulation, 2018* perhaps presently provides the most comprehensive definition of consent in that regard. Article 4(11) defines consent as that of the *Data Subject* that is “freely given” and constitutes the “specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.” It will of course depend on the context in which any particular piece of legislation or regulation is drawn up whether a fine tuning of this definition is required to further bring in a higher consensual threshold in the form of an *explicit* consent requiring a more exacting level of alertness, caution and transparency on the part of *Data Controllers* and *Processors* dealing in sensitive personal data especially in the realm of judicial and State functions. (See, “*India Draft Personal Data Protection Bill, 2018 & EU General Data Protection Regulation: A Comparative View – Deloitte*”).

The overriding objective of such regulatory régime is of course trust, i.e., trusting the State or other authorized entities to safeguard and protect all aspects of a natural person’s digital life in accordance with law. In this context, it cannot be gainsaid that an aspect of that protecting mechanism will also be to shield a digital life from unwarranted, unilateral, underground, and exploitative dealings in personal data. In other words, a natural person’s **digital footprints** cannot by any device be generated or duplicated to tread any farther than that intended by the *Data Principal* or *Subject*. A derogation from that intent will invariably be in breach of express consent given by such *Data Principal* and chip away at the fiduciary element fundamental in holding together the tripartite relationship I have earlier identified.

If emerging standards of data protection recognize a *Data Principal’s* right to the erasure of personal data concerning him or her and to that extent such part of a person’s digital life to be forgotten (the EUGDPR, 2018 in fact recognizes the right to erasure as coextensive with the “right to be forgotten”) then there is also the realization that such core guarantee to a person’s right to data privacy

can be made illusory by yet a fourth category of actors, the “*data brokers*” or “*data traffickers*”. I would argue that this category of purveyors or chains of purveyors in personal and highly vulnerable data remain a major irritant, if not a hurdle, to the sustainability of the regulatory régime we speak of. (Note that *The Global Risks Report 2020*, a *World Economic Forum* publication, identifies the **data brokering market** thriving on 4ir technologies and IoT devices and involved in “*the aggregating, disaggregating, copying, searching and selling data for commercial purposes*” to be worth an estimated US\$200 billion a year)

Operating outside of the tripartite or trinity of fiducial relationship discussed earlier, these brokers in personal data buy, acquire and sell data down a shadow chain of dealers engaging in packaging information for the next broker operating, often clandestinely and invisibly, down that chain. The fear is that beyond a certain point the chain operates virtually undetected and unregulated. The call now is for these *data traffickers* to be brought within a regulatory net. As Tim Cook in a January 2019 *TIME* magazine op-ed remarked in the US context,

“we believe the Federal Trade Commission should establish a data-broker clearinghouse, requiring all data brokers to register, enabling consumers to track the transactions that have bundled and sold their data from place to place, and giving users the power to delete their data on demand, freely, easily and online, once and for all.”

The relationships so defined in fact draw on pre-existing principles in vogue since the 1960s concerning collection and handling personal information. We, therefore, have the *Collection Limitation Principle* (requiring lawful collection of personal data by fair means with consent), *Purpose Specification Principle* (ensuring collection for purposes specified on the date collected and any subsequent use to be confined to such purpose or those compatible with prior notice given for projected use for an altered purpose), *Use Limitation Principle* (prohibiting use, disclosure and transfer of personal data except for disclosed purpose other than by consent of the *Data Subject* or by authority of law), *Security Safeguards Principle*

(deterring unauthorized access, destruction, use, modification or disclosure), *Openness Principle* (a transparent system of purpose of use and identity, for example, of the *Data Controller*), *Individual Participation Principle* (ensuring the *Data Subject's* access readily to his/her digital footprints and notably challenge data with a view to rectification, completion or erasure) and the self-evident *Accountability Principle* attaching to a *Data Controller*. (See, David Baniser, “*The Right to Information and Privacy: Balancing Rights and Managing Conflicts*”, 2011: World Bank Institute)

As we all appreciate, the writing is clearly on the wall regarding looming protection crises meriting firm and aggressive intervention by the law.



A legal régime protective of an individual's data ownership rights is like a customs check operating on a digital expressway.

DEMOGRAPHIC AND BIOMETRIC IDENTITIES

It is accepted as a given that the singularity of position of certain kinds of rights in a human rights narrative in this field of enquiry is unavoidable.

The entire range of concepts revolving around the notion of ownership of a person's data presciently came to be anticipated

in the dissenting opinion in the 2018 Indian Supreme Court Aadhaar Case dissecting the constitutionality of the *Aadhaar Act, 2016*. The majority decision upheld the constitutionality of the legislation as a whole barring certain provisions including section 57 that permitted use of Aadhaar information by mobile phone operators and banks.

The Aadhaar Act which aims at the delivery and availability of essential services on the basis of demographic and biometric identities collected, stored and shared, was challenged as violating the right to privacy. That challenge was dismissed by the Supreme Court generally.

Finding himself in disagreement with the majority view, Justice D. Y. Chandrachud echoed in an anticipatory view the emerging ideas of the fiduciary relationship binding the *Data Trinity*. This was evident starkly in his reservations on the validity, in particular, of section 57 of the Act in that, in his view allowing private entities to use Aadhaar numbers, under section 57, will lead to commercial exploitation of the personal data of individuals without consent and could also lead to individual profiling. *Justice Chandrachud warned that "these preferences could also be used to influence the decision making of the electorate in choosing candidates for electoral offices. This is contrary to privacy protection norms. Data cannot be used for any purpose other than those that have been approved."*

Justice Chandrachud's stress in his dissenting verdict on the singularity of the rights to ownership and

privacy is far-sighted and exposes why section 57 proves to be such a perilous proposition.

Predicated on his understanding that the architecture of the *Aadhaar Act* negates the fundamental principle that ownership of an individual's data must at all times vest with that very individual and no other, Justice Chandrachud emphasized that

"adequate norms must be laid down for each step from the collection to retention of biometric data based on informed consent, along with specifying the time period for retention. Individuals must be given the right to access, correct and delete data. An opt-out option should be necessarily provided."

Agreeing with the Petitioners, he found 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'*.

DATA PROTECTION RÉGIME IN BANGLADESH: THE BASIC TOOLS – CONSTITUTIONAL AND LEGISLATIVE

Article 43 of the Constitution: Protection of home and correspondence. 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.

Digital Security Act, 2018

Section 26) Punishment for Collecting, Using Identity Information without Permission, etc.: -

২৬। (১) যদি কোনো ব্যক্তি আইনগত কর্তৃত্ব ব্যতিরেকে অপর কোনো ব্যক্তির পরিচিতি তথ্য সংগ্রহ, বিক্রয়, দখল, সরবরাহ বা ব্যবহার করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপ-ধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৫ (পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ৫ (পাঁচ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

(৩) যদি কোনো ব্যক্তি উপ-ধারা (১) এ উল্লিখিত অপরাধ দ্বিতীয় বার বা পুনঃপুন সংঘটন করেন, তাহা হইলে তিনি অনধিক ৭ (সাত) বৎসর কারাদণ্ডে, বা অনধিক ১০ (দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

ব্যাখ্যা।- এই ধারার উদ্দেশ্য পূরণকল্পে, “পরিচিতি তথ্য” অর্থ কোনো বাহ্যিক, জৈবিক বা শারীরিক তথ্য বা অন্য কোনো তথ্য যাহা এককভাবে বা যৌথভাবে একজন ব্যক্তি বা সিস্টেমকে শনাক্ত করে, যাহার নাম, ছবি, ঠিকানা, জন্ম তারিখ, মাতার নাম, পিতার নাম, স্বাক্ষর, জাতীয় পরিচয়পত্র, জন্ম ও মৃত্যু নিবন্ধন নম্বর, ফিংগার প্রিন্ট, পাসপোর্ট নম্বর, ব্যাংক হিসাব নম্বর, ড্রাইভিং লাইসেন্স, ই-টিআইএন নম্বর, ইলেকট্রনিক বা ডিজিটাল স্বাক্ষর, ব্যবহারকারীর নাম, ক্রেডিট বা ডেবিট কার্ড নম্বর, ভয়েজ প্রিন্ট, রেটিনা ইমেজ, আইরিস ইমেজ, ডিএনএ প্রোফাইল, নিরাপত্তামূলক প্রশ্ন বা অন্য কোনো পরিচিতি যাহা প্রযুক্তির উৎকর্ষতার জন্য সহজলভ্য।

(1) If any person **without any legal authority** collects, sells, takes possession, supplies or uses any person's **identity information**, then, that activity of that person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5(five) years or fine not exceeding 5 (five) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be penalized with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both.

Explanation: -

To fulfill the objective of this Section, **“Identity Information”**, means any external, biological or physical information or any other information which singly or jointly can identify a person or a system, his/her name, address, Date of birth, mother's name, father's name, signature, National identity, birth and death registration number, finger print, passport number, bank account number, driver's license, E-TIN number, Electronic or digital signature, username, Credit or debit card number, voice print, retina image, iris image, DNA profile, Security related questions or any other identification which due to the excellence of technology is easily available.

NEED FOR JUDICIAL INTERVENTION

Given the primary tools of data protection as above identified, it is with a sense of urgency, therefore, that I introduce this segment of my views on the subject matter and convey how these may be applied to the optimum.

Public Interest Litigation (PIL) emerges at this juncture as a feasible mode of intervention to secure a balance between the notions of 'security' and 'protection', or rather, national security and personal protection. The answer lies, in my opinion, in the very molecular structure of this mode of legal agitation. That structure has been defined by PIL interventions over the years. I provide hereinbelow a checklist of the essential attributes

and strengths of PIL as inure to its effectiveness for bringing about the 'balance' I speak of. Exertions made and avenues explored in two of my own decisions, if I may emphasize, are declaratory of the pragmatic measures that the Judiciary can itself initiate to engage constructively and fruitfully with the Executive in upholding a rights-based perspective. The two judgments I speak of were delivered in (i) **Syed Saifuddin Kamal vs. Bangladesh, Ministry of Health** (Writ Petition No. 1509 of 2016; Judgment delivered on 8.8.2018) reported in 38 BLD (2018), 453 and (ii) **Human Rights and Peace for Bangladesh vs. Bangladesh** (Writ Petition No. 14258 of 2012; Judgment delivered on 25.4.2019).

An enlightening analysis of the essential core features of PIL is to be found in Justice P. N. Bhagwati's analysis in ***People's Union for Democratic Rights vs. Union of India*** (1982 AIR SC, 1473).

These features may be identified thus:

- PIL is a different kind of litigation from the ordinary traditional litigation which has an adversary character.
- PIL is intended to promote and vindicate public interest which demands that violations of constitutional or legal rights of a large group of disadvantaged people do not go unnoticed and unaddressed.
- Correcting a wrong or filling legal and administrative lacuna require multi-dimensional strategies including ***PIL which is a cooperative or a collaborative effort*** on the part of the petitioner, State or public authority ***and the Court*** to secure the observance of constitutional or legal rights.
- ***The State or public authority against whom PIL is brought should be as much interested*** in ensuring basic rights as the petitioners and the generally disenfranchised.
- ***The State or public authority*** which is arrayed as a respondent in PIL ***should, in fact, welcome it, as it gives it an opportunity to right a wrong.***

These strands of thought constituting the rationale behind PILs found fruition in ***Syed Saifuddin Kamal vs. Bangladesh, Ministry of Health (Writ Petition No. 1509 of 2016; Judgment delivered on 8.8.2018) : 38 BLD (2018), 453*** in which the court through a collaborative exercise spurred and guided the formulation of the ***“Emergency Medical Services for Road Accident Victims and Protection of Good Samaritans Policy, 2018”*** সড়ক দুর্ঘটনায় আহত ব্যক্তির জরুরী স্বাস্থ্য সেবা নিশ্চিত করণ ও সহায়তা কারীর সুরক্ষা প্রদান নীতিমালা, ২০১৮. Article 9 of the ***National Road Safety Strategic Action Plan (“NRSSAP”) 2014-2016*** constituted a starting point for requisite action in this case. The Court noted, however,

that while article 9 provides for measures of first aid to be administered to road accident victims it *“contains no clear directions regarding the exact nature, kind and extent of services to be provided or indeed how to regulate or monitor compliance in providing emergency services.”*

Accordingly, the Court proceeded to fill that lacuna through a very much cooperative and collaborative effort bringing all stakeholders on board and aiding the concerned public authority and the State to adopt and implement concrete measures in the area of emergency medical care for road accident victims.

As noted by the Court in the Syed Saifuddin Kamal Case the নীতিমালা *“is an outcome of strident, bold and trail-blazing efforts of all stakeholders concerned and chiefly the two Petitioners (Petitioner No. 2 being BLAST & the Respondent No. 1, Ministry of Health).”*

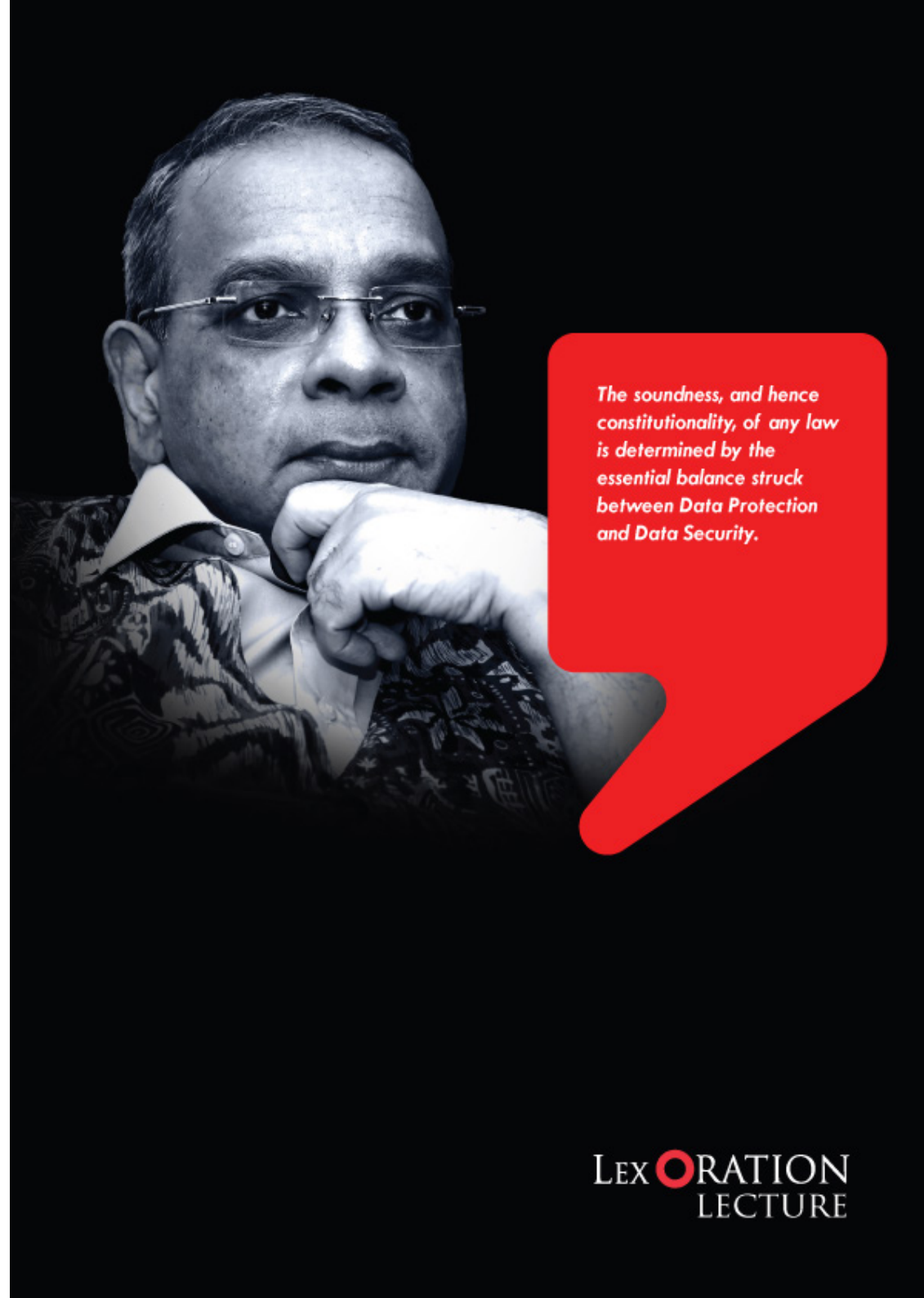
Care was taken by the Court not to overreach its constitutional mandate

in the dispensation of justice and not to encroach into the Executive's sole domain of policy-making and the Legislature's authority to make law. This is reflected in the Court's refrain at the end of the judgment clarifying that the *“নীতিমালা in its entirety be deemed enforceable as binding by judicial sanction and approval pending appropriate legislative enactments incorporating entrenched standards, objectives, rights and duties.”*

In ***Human Rights and Peace for Bangladesh vs. Bangladesh (Writ Petition No. 14258 of 2012, Judgment delivered on 25.4.2019)*** the petitioners sought the Court's intervention with a view to a systemic overhaul and upgradation of regulatory frameworks to ensure the installation and functioning of Mobile Phone Towers (MPTs) in a sustainable manner eliminating risks of undue exposure to the harmful public health effects of their operation, i.e., they pose imminent a grave danger to public health.

The respondent No. 4, Bangladesh Telecommunication Regulatory Commission (BTRC) drew on its powers to issue necessary directions under various provisions of the *Bangladesh Telecommunication Regulatory Act, 2001* and the Court relied on the Government's authority under section 34(2) of that Act to make guidelines. The Government had notably empowered the BTRC to formulate the "*Guidelines for Limiting Exposure to Radiation of Electromagnetic Fields (9 Khz to 300 Ghz)*". Significantly, the Court resorted to the vehicle of the method of Continuing Mandamus, thereby, ensuring a continued engagement of all stakeholders to put together a sustainable regulatory mechanism. In this regard, the Court noted

that "*precautionary approach must inform our comparative analysis of the sufficiency of the Guidelines and the feasibility of their implementation to attain a desired objective.*" Thus, the Court remarked that it "*by way of abundant caution, and necessarily so, has desisted from readily sanctioning a quick fix to a complex scenario. The objective henceforth is for progressive developments and a greater holistic approach towards the finalizing of the Guidelines with the dominant and overarching objective of serving the public interest and safeguarding public health.*"



The soundness, and hence constitutionality, of any law is determined by the essential balance struck between Data Protection and Data Security.

EPILOGUE

Predicated on the above, the need for drawing a distinction between data protection and data security becomes starkly compelling in the context of The *Digital Security Act, 2018*. This is because there is a notable absence in the 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 when pitted against the demands of data security. That in turn leaves the protection narrative to fall by the

wayside, at least for the time being. By definition, the concept of digital security in the Act encompasses the protection of databases and systems or, in other words, prevention of unwanted and unauthorized access to or use of databases, in the overriding interest of safeguarding national digital security. This is not to be confused with personal data protection as discussed earlier. That aspect of protection receives limited treatment only in section 26 of the Act.

But section 26 in incorporating the concept of “legal authority” regarding use of personal data stops short of identifying the concepts of “privacy” and “consent” in particular. It is to be noted, however, that while the term “legal authority” is not a defined one under the Act, the act of “illegal entrance” is and it is in that latter instance, for example, that the notion of consent or permission crops up thus:

২। সংজ্ঞা।- (১) বিষয় বা প্রসঙ্গের পরিপন্থি কোনো কিছু না থাকিলে এই আইনে-
(খ) “বে-আইনি প্রবেশ অর্থ কোনো ব্যক্তি বা কর্তৃপক্ষের অনুমতি ব্যতিরেকে বা উক্তরূপ অনুমতির শর্ত লঙ্ঘনক্রমে কোনো কম্পিউটার বা ডিজিটাল ডিভাইস বা ডিজিটাল নেটওয়ার্ক বা ডিজিটাল তথ্য ব্যবস্থায় প্রবেশ, বা উক্তরূপ প্রবেশের মাধ্যমে উক্ত তথ্য ব্যবস্থার কোনো তথ্য-উপাত্তের অদান-প্রদানে বাধা প্রদান বা উহার প্রক্রিয়াকরণ স্থগিত বা ব্যাহত করা বা বন্ধ করা, বা উক্ত তথ্য-উপাত্তের পরিবর্তন বা পরিবর্ধন বা সংযোজন বা বিয়োজন করা অথবা কোনো ডিজিটাল ডিভাইসের মাধ্যমে কোনো তথ্য-উপাত্ত সংগ্রহ;

2) *Definition:* -

(1) *Unless there is anything repugnant in the subject or context, in this Act, ...*

q) “*Illegal Entrance*” means entrance without the permission of any person or authority or entrance in violation of the conditions of permission

of entrance by the said person or authority into any computer or digital device or digital network system, or by above mentioned entrance create hindrance in the exchange of any data-information suspend or prevent or stop the process of exchange of data-information, or change the data-information or add or deduct the data-information or collect the data-information with the use of a digital device.

Indeed, the Act does not bear reference to the *Digital Trinity* or the tripartite relationship as discussed earlier. Consequentially, there are no rights enumerated specifically inuring to the benefit of a *Data Principal* or *Subject vis-à-vis* the roles and duties assigned to *Data Fiduciary* or *Collector*, and *Data Processors*. Nor does the problem of data brokering get any coverage in the Act.

The pathways of remedial intervention to address such inadequacy or lacuna within the Act's scheme may at best be identified through the rule-making authority under section 60:

যেহেতু ডিজিটাল নিরাপত্তা নিশ্চিত করণ এবং ডিজিটাল মাধ্যমে সংঘটিত অপরাধ শনাক্ত করণ, প্রতিরোধ, দমন, বিচার ও আনুষঙ্গিক বিষয়াদি সম্পর্কে বিধান প্রণয়ন করা সমীচীন ও প্রয়োজনীয়;

৬০। বিধি প্রণয়নের ক্ষমতা। এই আইনের উদ্দেশ্য পূরণ কল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, বিধি প্রণয়ন করিতে পারিবে।

(২) উপ-ধারা (১) এর সামগ্রিকতাকে ক্ষুণ্ণ না করিয়া, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, অন্যান্য বিষয়ের মধ্যে, বিশেষত নিম্নবর্ণিত সকল বা যে কোনো বিষয়ে বিধি প্রণয়ন করিতে পারিবে, যথা:-

- (ক) ডিজিটাল ফরেনসিক ল্যাব প্রতিষ্ঠা;
- (খ) মহাপরিচালক কর্তৃক ডিজিটাল ফরেনসিক ল্যাব তত্ত্বাবধান;
- (গ) ট্রাফিক ডাটা বা তথ্য পর্যালোচনা এবং উহা সংগ্রহ ও সংরক্ষণ পদ্ধতি;
- (ঘ) হস্তক্ষেপ, পর্যালোচনা বা ডিক্রিপশন পদ্ধতি এবং সুরক্ষা;
- (ঙ) সংকটাপন্ন তথ্য পরিকাঠামোর নিরাপত্তা;
- (চ) ডিজিটাল নিরাপত্তার ক্ষেত্রে আঞ্চলিক ও আন্তর্জাতিক সহযোগিতার পদ্ধতি;
- (ছ) ইমার্জেন্সি রেসপন্স টিম গঠন, পরিচালনা ও অন্যান্য টিমের দলের সহিত সমন্বয় সাধন;
- (জ) ক্লাউড কম্পিউটিং, মেটা ডাটা; এবং

(ঝ) সংরক্ষিত ডাটা'র সুরক্ষা।

Whereas it is expedient and necessary to formulate an Act for ensuring National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters

60) The power to make rules: -

- (1) *To fulfill the objective of this Act, government, by notification in the government gazette, can enact rules.*
- (2) *Without prejudice to the subsection (1), government by notification in the government gadget, can enact rules for especially for the following among other subjects namely: -*
 - a. *Establishing Digital Forensic Lab;*
 - b. *Supervision of the Digital forensic Lab by the Director General;*
 - c. *Reviewing traffic data or information and the process of its collection and preservation;*

- d. *Process of Interference, Review or Decryption and Protection;*
- e. *Security of Compromised Information Infrastructure;*
- f. *The process of Regional and International Assistance in terms of Digital security.*

A cautionary note is, however merited here. Realistically, protection rules may not sit comfortably in a statutory scheme that is not premised on a rights-based approach. That leaves us in a protection deficient system with few or some statutory tools to build on from a protection perspective. We, therefore, find ourselves in a profound crossroads. Time now, accordingly, to rethink and reorient ourselves on the issue of personal digital protection taking inspiration from initiatives far and near.

Fundamentally yet, the advent of 4ir shall demand a reorientation of legislative and judicial perceptions of the Rule of Law. For it is inevitable, that substantive democracies and aspirants alike shall be constrained to redefine not only the contours, for example, of the protection of home and correspondence (as under article 43 of our Constitution) but significantly the right to be secured by and under the law (as under article 31 of the Constitution) to neutralize the disruptive traits of 4ir and negate the invasive utilization of the same for extra-constitutional purposes.

BIBLIOGRAPHY

Books and Reports

- Brad Smith, Carol Ann Browne “Tools and Weapons: The Promise and the Peril of the Digital Age”, 2019: Hodder & Stoughton
- David Baniser, “The Right to Information and Privacy: Balancing Rights and Managing Conflicts”, 2011: World Bank Institute)
- Global Risks Report 2020: Insight Report -15th Edition: World Economic Forum

Legislation

- Digital Security Act, 2018
- Bangladesh Telecommunication Regulatory Act, 2001
- India Draft Personal Protection Bill, 2018
- EU General Data Protection Regulation (EUGDPR), 2018
- The Universal Declaration of Human Rights
- Charter of Human Rights and Principles for Internet
- The European Union Data Protection Directive

Case Laws

- Human Right and Peace for Bangladesh vs. Bangladesh
- Syed Saifuddin Kamal vs. Bangladesh, Ministry of Health
- People’s Union for Democratic Rights vs. Union of India
- People’s Union of Civil Liberties (PUCL) vs. Union of India & Ors.
- Justice K. S. Puttaswamy (Retd) vs Union Of India

Websites

<https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-scheme-does-not-violate-right-to-privacy-says-sc/articleshow/65969846.cms?from=mdr>

http://www.lawphil.net/judjuris/juri2008/jan2008/am_08-1-16_sc_2008.html).

<http://www.wpfc.org/index.php?q=node/221>.

<https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-petitioner-justice-ks-puttaswamy-welcomes-supreme-court-verdict/articleshow/65974044.cms?from=mdr>

<https://www.livemint.com/Politics/M5yPbMI8duh31IHVUvOIPP/Aadhaar-supreme-court-verdict-uidai-bank-account-mobile-link.html>

<https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>

©BANGLADESH INTELLECTUAL PROPERTY FORUM, 2020

CREATIVE DESIGNER: MUNSI ARAF
AGENCY: ZERO SPACE EXPERTS
PHOTOGRAPHER: MD. SHAKHAWAT

A PUBLICATION OF
BANGLADESH INTELLECTUAL PROPERTY ACADEMY

LEX  ORATION



LEXORATION



0101 28012020