About Author

Dr. Anala Andini is a distinguished academician and orator having presented more than 100 invited lectures, workshops and seminars. She has an outstanding career with a wide range of experience in teaching and research. Having received her formal schooling in Kannada medium, she holds degree in law from Mangalore University. Dr. Anala received Ph.D. in Women and Law from Kuvempu University. In the backdrop of long years of experience in legal literacy, She has more than 26 years of teaching experience. Her teaching and research interests include Jurisprudence, Constitutional Law, Human Rights, Teaching and Research Methodology, Women and Law, Environmental Law, besides guiding Masters and Ph.D students. Dr. Anala has more than 20 articles and book chapters to her credit.

978-81-985864-3-8

CRDEEP Publications

Rajendranagar, Dehradun, Uttarakhand India
Premier Publishers of Journals and Books
E mail: editor@crdeepjournal.org
Call us at: 7895844394
Visit our store at: www.crdeepjournal.org

RIGHT TO PRIVACY

IN THE ABSENCE OF

DATA PROTECTION REGIME IN INDIA

1st Edition 2021

ISBN: 978-81-985864-3-8

Dr. ANALA A

CRDEEP PUBLICATIONS

ISBN: 978-81-985864-3-8

RIGHT TO PRIVACY IN THE ABSENCE OF DATA PROTECTION REGIME IN INDIA

By:

Dr. ANALA A

Associate Professor

C.B.R College of Law and Centre for Post Graduate Studies, Shivamogga

CRDEEP PUBLICATIONS

2021

FOREWORD

Privacy and Data Protection are essential concepts in modern digital communication and information-sharing. The book looks into how with the increasing use of technology in our daily lives, we generate vast amount of data that can be collected, stored, analysed, and shared by various entities, as happened in the Facebook and CA scandals. What India has done so far to protect an individual's privacy, both Parliament and Supreme Court. The book also discusses the limits that can be imposed on the right to privacy and how this right is developed and protected in U.K. and U.S.A. How international covenants and conventions are protecting the right to privacy. Understanding what privacy and data protection entail and why the matter is essential. First of all, I would like to warmly congratulate the Publishers and the Editors, CRDEEP Publishers on their initiative in bringing together – for the first time – between the covers of this Book a wealth of information and expertise across the nation on the creation and legal protection of the right to privacy. Privacy and Data Protection delves into the evolving importance of privacy in today's interconnected world. As the digital age expands, the book emphasizes the need to safeguard personal data, aligning with the growing significance of privacy as a fundamental human right. It explores key legal frameworks like India's Digital Personal Data Protection Bill (2023), which enhances individual control over personal information, ensuring transparency and accountability. This volume is a valuable resource for students, researchers, and legal professionals, offering an in-depth analysis of the challenges and legal frameworks shaping data privacy in the modern world. Privacy is an important human right enshrined in many international treaties. It is essential for the protection of human dignity and is one of the solid pillars of a democratic country. The right to life within Article 21 is freely interpreted and therefore, it includes all aspects that makes a person’s life more meaningful. The concerned State authorities have passed numerous laws to protect the privacy of their subjects. However, these measures are not impenetrable and are restricted in some circumstances by the government. As more information is digitized and shared online, the need for data protection and privacy is growing. Data must be managed based on its perceived relevance since people care deeply about the privacy of their personal information. Along with that, technology is a sector which is growing every single minute and hence extensive discussion on this topic is the need of the hour. The book delves into all these significant aspects.

G R Jagadeesh
PRINCIPAL
CBR National College of Law
SHIMOGA-577 201

ACKNOWLEDGEMENT

With immense pleasure and gratitude, I duly acknowledge the assistance and support received from various people who paved way for the completion of this research work.

Words cannot express my gratitude to my teachers and mentors for their invaluable patience and feedback. I also could not have undertaken this journey without my Guru, who generously provided knowledge and time. Additionally, this endeavour would not have been possible without the generous support from the primary data sources.

I am also grateful to my fellow teachers especially my college team, for their editing help, late-night feedback sessions, and moral support. Thanks should also go to the librarians, research assistants and study participants from the university, who impacted and inspired me.

Lastly, I would be remiss in not mentioning my family, especially my parents, spouse, and children. Their belief in me has kept my spirits and motivation high during this process. I would also like to thank my pet for all the entertainment and emotional support.

TABLEOFCONTENTS

CHAPTER1:INTRODUCTION

1.1 India and the Need for Data Protection

It is often said that Data is the new oil[1]. With an intensely digitalized world and an increasingly digitalized India, the significance assumed by the data has reached unprecedented heights in the last couple of decades. The motive behind most of the cybersecurityattacksinIndiaintherecentpasthasbeenaimedatstealingdata.There have been numerous instances of health data[2], financial data[3] and other important personal[4] and sensitive data[5] being compromised by the cyber attackers. Numerous instances of data breaches including the hacking of social media accounts[6], theft of creditanddebitcarddetailsandotherprivacybreachesgounreportedduetothelack of stringent data protection laws in Indiathat could afford adequate protection to the sensitive and personal data of the citizens in the recent past.

In an investigative report published by The Tribune Newspaper in the year 2018, made a sensational claim that entire Aadhar Database (containing personally identifiable information of over 1.3 billion Indians) could be accessed by paying a meagre sum of 500 INR[7].The Aadhar breach was rightly described as the world's biggest data breach so far by think-tanks and the global media. Further, a report publishedbydigitalsecurityfirmGemaltoclaimedthatIndiaaccountsforover37%

[1]NANDANKAMATH,LAWRELATINGTOCOMPUTERS,INTERNET,ANDE-COMMERCE:AGUIDETOCYBERLAWS AND THE INFORMATION TECHNOLOGY ACT, 2000 121 (1STED. 2020)

[2]*Id.*

[3]*Id.*

[4]PAVANDUGGAL,CYBERSECURITYLAW42-103(1STED.2019)

[5]Jason Asbury, Maria McClelland , Kris Torgerson, India Vincent & Jennifer Boling, *Law and BusinessTechnology:CyberSecurity &DataPrivacyUpdate*,20Transactions: TENN.J. BUS. L. 1065, 1067-71 (2019).

[6]*Id.*

[7] R. Khaira, *Rs 500, 10 Minutes, And You Have Access To Billion Aadhaar Details*.TRIBUNE INDIA NEWS SERVICE, (Nov, 2018.): <https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

of the global data breaches[8] and is second only to the United States in terms of the databreach[9].Thefrequentbreachofdatainanincreasinglydata-driveneconomyhas highlighted the void created by the non-existence of a robust data protection framework in India.

ThisStudyhasbeentakenupwiththespecificobjectiveofstudyingtheexistingand upcoming data protection law in India while comparing it with the laws in advanced data protection regimes in order to highlight the lacunas in our data protection framework. The law of data protection is of particular concern to India due to innumerable factors, the most prominent of them being the extensively vast populationofIndia[10].Indiahasover500millionInternetusersandthecountgrowing at arateofover8%per annum; itisby farthebiggest market in the digitaleconomy as of today. With the digital economy in India headed towards an unprecedented boom[11],itmaysoonbecomeaveryimpendingchallengetoaddresstheissuesarising out of voluminous transactions in the form of the digital medium.

In the recent past, India has also witnessed a fillip in the use of digital space in the sectoroffinanceandwithaninfluxofmoreadvancedtechnologiesandanaggressive posturefromthegovernmenttopromotedigitaltransactionsafterthedemonetization, hasmadetheuseofdataevenmoresignificantandpronetomisuseatthesametime[12]. The growth in usage of online platforms like Google Pay, BHIM, Paytm and numerous other start-ups facilitating digital transactions[13] are testimony to the fact thattheIndianshaveenteredintoanagewherethesedigitalmediumshavebecome

[8]DhirajR.Doraiswamy,*PrivacyandDataProtectioninIndia*,6J.L.&CYBERWARFARE166, 169-172 (2017).

[9]*Id.*

[10]SSingh,*PrivacyandDataProtectionInIndia:ACriticalAssessment*,53JOURNALOF THE INDIAN LAW INSTITUTE,104-111(2012).

[11]NMathur,*IndiaNowHasOver500MillionActiveInternetUsers:IAMAI*.LIVEMINT(Jan 2020)<https://www.livemint.com/news/india/india-now-has-over-500-million-active-internet-users-iamai-11588679804774.html>

[12]*Id.*

[13]*Id.*

an indispensable aspect of our lives and thus there needs to be a strong and effective mechanism in place in order to provide adequate security to these transactions[14].

With the penetration of high-speed Internet within the nooks and corners of the country, the threat to the informational privacy looms larger than ever now.[15] While the digitalization of the economy has opened the way for a plethora of job opportunitiesinthesectorspertainingtoHealth,EducationandGovernance,theneed to have a strong law in place in order to ensure maximum protection to these personally sensitive data of the individuals becomes more important than ever.

1.2 Locating the Meaning of Data Protection

DataProtection has been defined as oneofthemost abstract concepts in thelawthat isbereftofbeingascribedaone-linedefinition.Juristshaveopinedthattheterm"data protection" is a catch-all terminology that is used to denote everything that is associated with the processing of personal data[16].The first ever data protection law – Sweden'sDataAct–waspassednearly50yearsago,in1973,andcameintoeffect the following year. The Swedish Data Protection Authority made it illegal for any person or company to use information systems of any kind to handle personal data withoutalicense.Inthelate60s,citizensoftheprogressiveScandinaviannationhad become concerned about the growing use and storage of personal data, and the Data Act was conceived to allay their fears.

Dataprotectionreferstothepractices,safeguards,andbindingrulesputinplace toprotectyourpersonalinformationandensurethatyouremainincontrolofit. Inshort,youshouldbeabletodecidewhetherornotyouwanttosharesome

[14]Dhiraj R. Duraiswami, *Privacy and Data Protection in India*, J.L.&CYBERWARFARE 166, 169-72 (2017).

15*SCnoticeonprivacyconcernstoGoogle,WhatsApp,Amazon*,HINDUSTANTIMES, UPIshttps://www.hindustantimes.com/india-news/sc-notice-on-privacy-concerns-to-google-whatsapp-amazon-upis-101612192948826.html,

[16]David Wallace &Mark Visger, *Responding to the Call for a Digital Geneva Convention: An OpenLettertoBradSmithandtheTechnologyCommunity*,6J.L.&CYBERWARFARE3,12-13 (2018).

information, who has access to it, for how long, for what reason, and be able to modify some of this information, and more.

Two prongs of the data protection laws, that go on to build the lion's share of the meaning of data protection laws are "personal data" and "processing"[17]. These two concepts are focal to the analysis of the underlying rationale behind the data protection laws and hence require a considerable degree of attention[18]. The term processingisaswideastheentirelawofdataprotectionitselfandthusitoughttobe construed liberally in order to broaden the ambit of the protection conferred by it[19]. The term processing refers to any material activity that has a direct bearing on the data and this would go on to include, collection of data, its storage, its erasure, its usage, its dissemination[20].

Most of the advanced data protection regimes favour giving the widest possible meaningtotheterm. It hastobeacceptedthat alooselydefinedmeaning oftheterm "processing"wouldgoontovitiatetheverypurposebehindhavingadataprotection law[21].The second aspect of the Data Protection Laws is of course the concept of "Personal Data."[22] The term refers to anything that can be used to identify a person or any information that can be linked to the individual identity of a person[23]. Followingthis very lineof reasoning, thecourtsin the European Union haveapplied

[17] *Id.*

[18] *Id.*

[19] UmangJoshi, *OnlinePrivacyandDataProtectioninIndia:ALegalPerspective* ,7 NUALS L.J. 95, 101-103 (2013).

[20] *Id.*

[21] Alibeigi, Ali, "*Towards Standard Information Privacy, Innovations of the new General Data ProtectionRegulatio*n"LIBRARYPHILOSOPHYANDPRACTICE(E-JOURNAL),2840,(2019).. https://digitalcommons.unl.edu/libphilprac/2840whereintheauthorassertsthatthe personaldata protection law is about individual's right to control his/her information while highlighting the approachoftheEuropeanJurisdictionsintreatingtheright toprivacyasaconcomitantofrightto life.

[22] *SeeDBruschi,Informationprivacy:NotjustGDPR,* PHILOSOPHICALENQUIRY(CEPE) PROCEEDINGS, (9 pp.).

[23] LathaR.Nair, *DataProtectionEffortsinIndia:BlindLeadingtheBlind*, 4 INDIAN J. L. & TECH. 19, 21-22 (2008).

the test of "personally identifiable" information for determining whether a class of data can be classified as personal or not[24].

With theseprongs mystified, onegets into position to havea clearer pictureofthe conceptofdataprotectionlaws.Thatbeingnoted,onecanformulatethedefinitionof dataprotectionlawsas,asetofrulesthatprotectthedissemination,collection,using, erasure, storage and destruction of all the information that can be used to identify a person. Here protection implies a reasonable degree of fairness in the processing of personaldatathatconformstotheestablishedprinciples[25].However,thelawsofdata protectionhavecomealongwayfrommerefairprocessingofpersonaldataandnow referstoamorejurisprudentiallyevolvedconceptofinformationalself-determination and informational autonomy[26]. The term informational self-determination refers to the right of the individual to decide the terms on which the personal data can be disclosed in the first place[27].

1.3 The Right to Data Protection and Rule of Law

Therightofinformationalself-determinationhascometobeconsideredasaninherent aspect of the rule of law. It has been opined that the lack of adequate autonomy in exercising informational self-determination "*would also impair the common good becauseself-determinationisanelementaryfunctionalconditionofafreedemocratic community[28]*". This assertion springs from the fact that Data Protection is at times consideredasanoffshootoftherighttoprivacy[29].However,amajorportionofthis

[24]VinitaBali, *DataPrivacy,DataPiracy:CanIndiaProvideAdequateProtectionfor Electronically Transferred Data*, 21 TEMP. INT'L & COMP. L.J. 103, 109-10 (2007).
[25]Sougata Talukdar, *Privacy and Its Protection in Informative Technological Compass in India*, 12 NUJS L. Rev. 1 (2019).
[26]HenryPearce, *SystemsThinking,BigData,andDataProtectionLaw*,18 Eur.J.L.Reform478 (2016).
[27]*Id.*
[28]*Id.*
[29]*Id.*

debateisconfinedtotheEuropeanConstitutionalCourtsandhencewillbedealtwith in detail at the appropriate stage.

Asalreadynoted,theconceptofdataprotectionhasevolvedfromthestateofbeinga tool to protect the unwarranted inferences with the sensitive and personally identifiable information of the citizens, to be a central aspect of the social order that considers the right to informational self-determination as indispensable character of every society governed by rule of law[30].

1.4 Right to Privacy and Its Relation with Data Protection

Therecanbenodenialofthenormativefactthatthereexistsanunfetteredcorrelation between right to privacy and the data protection law. Howsoever different these two nebulous concepts may be from each other theoretically, the relation between Right to Privacy and the Right to Data Protection is a concrete one[31]. The very argument that data protection laws have come such a long way to be considered as a fundamental right stem from thefact that the right to privacy has been recognized as one[32]. The Supreme Court of India, upon same lines, had directed the Central government to come up with a data protection code, only after it had identified the righttoprivacyasaninherentpartoftherighttolifeandlibertyasguaranteedbythe Article 21 of the Constitution of India[33]. That doesn't leave any doubt that the data protection legislations do have the intent to protect the right to privacy of the individuals at theirhelm[34]. However,in a countrylike India wherethejurisprudence ofrighttoprivacyisstillinitsinfancy,thereneedstobeacutanddrieddefinitionof the right to privacy for the purpose of the Data Protection legislation.

[30]OrlaLynskey,*DeconstructingDataProtection:TheAdded-ValueofaRighttoDataProtection in the EU Legal Order*, 63 INT'L&COMP. L.Q. 569, 577-81 (2014).

[31]Silvia Lucia Cristea &Viorel Banulescu, *The Right to Personal Data Protection. The Right to Privacy.AComparativeLawApproach*,64 ANALELESTIINTIFICE ALE UNIVERSITATII ALEXANDRUIOAN CUZADINIASISTIINTE JURIDICE1,03-05 (2018).

[32]*Id.*

[33]KSPuttaswamyv.UnionofIndia, 2017SCCOnlineSC 996

[34]SupraNote30at04

However, just as the Data Protection Law, the right to privacy is quite a nebulous conceptandthereexistsagreatdegreeofconfusionamongstthelegislaturesallover the world in giving out a concrete definition of the right to privacy[35]. However, in order to effectuate the very purpose of the data protection laws, there needs to be a concreteandrationaldefinitionoftherighttoprivacy.Thelimitednumberofjudicial precedents makes it imperative to rely upon some of the well-settled principles relating to it and more importantly, the data protection laws should themselves be broadenoughtolayoutintheclearestofterms,themeaningandscopeoftherightto privacy.

The failure to chalk out a precise definition of the right to privacy has its own costs and benefits. It may be an advantage in as much as the lack of a definition provides ample room for flexibility for the judiciary to interpret it in the widest sense[36]. The changing world of technology seems to reinvent itself each passing day and thus it maybein thebest interests ofthecitizens, thedemocraticframework and theruleof law to keep the understanding of the right to privacy as open-ended as possible[37]. There has been a great deal of debate as to what should be considered as the most precise definition of the right to privacy[38].

The voluminous literature pertaining to the relationship between the right to privacy and data protection laws purport to establish the link between the right to informational self-determination and information control[39]. One of the most quoted understandings oftheright to privacy in therealmofdataprotection is that"*Privacy istheclaimofindividuals,groups,orinstitutionstodetermineforthemselveswhen,*

[35]SupraNote30at05

[36]Edward J. Eberle, *The Right to Information Self-Determination*, UTAHL.REV.965, 969-971 (2001).

[37]*Id.*

[38]*Id.*

[39]Eva Fialova, *Data Portability and Informational Self-Determination*,8 MASARYK U. J.L. & TECH.45, 456-51 (2014).

how, and to what extent information about them is communicated to others[40]." The sole reason behind the popularity and the acceptance of this approach can be traced to the enormous appeal that the "right to self-determination" has over the people in any democratic set-up[41]. However, there's a need to reconcile with the fact that the *stricto senso* no data protection law can guarantee complete informational self-determination however, what a robust law can ensure is a regulated determination[42].

AmoreoldandyetpopularunderstandingoftheRighttoPrivacyhasbeenassociated withtherighttobeletalone.Thisapproachtreatsthenon-interferenceasaninherent part of the right to privacy. As per this version, three prongs of the right to privacy include, "secrecy, anonymity and solitude[43]." No discussion on the Right to Privacy caneverbecompletewithoutreferringtotheseminalworkofSamuelDWarrenand LouisD.Brandeisthatlaidthefoundationsofrecognitionof therighttoprivacyas a distinct right.

> *"These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to bemaliciouslyprosecuted,therightnottobedefamed.Ineachofthese rights,asindeedinallotherrightsrecognizedbythelaw,thereinheres the quality of being owned or possessed- and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But obviously, they bear little resemblance towhatisordinarily comprehendedunderthatterm.The*

[40] JakubMisek, *ConsenttoPersonalDataProcessing-ThePanaceaortheDeadEnd*,8 MASARYK U. J.L. & TECH.69, 71-72 (2014).
[41] *Id.*
[42] *Id.*
[43] *Id.*

principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality[44]."

Numerousdataprotectionprinciplesdotakeintoaccountthesefeaturestoensurethat thegreatestpossibleprotectionisgrantedtotheindividuals.Thegenesisofprinciples of data protection such as the principle of fairness of processing, the principle of purpose limitation and the right to erasure[45] can be traced to the conception of the right to be let alone.The yet another approach to connect right to privacy with Data protection is the disclosure of sensitive material[46].Sensitive materials are usually those data which have the tendency to expose the identity of the individuals such as name, sexual preferences, residential address etc. There is a great deal of disagreementamongstthescholarswithregardstotheeffectivenessofthisapproach as it is highly likely that through the technological advancements in this era of Big data, information that is not otherwise sensitive may be collected and processed in a way that would make them of sensitive character[47]. Keeping these aspects of these separate approaches about the nature of the right to privacy, the Supreme Court of India chose to adopt the informational self-determination approach:

"Aboveall,theprivacyoftheindividualrecognisesaninviolableright to determine how freedom shall be exercised. An individual may perceivethatthebestformofexpressionistoremainsilent.Silence

[44]Samuel D. Warren &Louis D. Brandeis, *Right to Privacy*, 4 Harv.L.Rev.193 (1890-1891). Louis was a professor at the Harvard Law School and a staunch advocate of the fundamental character of the Right to Privacy. This paper is considered to be the most authoritative literature on the developing cantors of Data Protection.

[45]Alina Savoiu&Catalin Capatina Basarabescu, *The Right to Privacy*, 2013 Annals Constantin Brancusi U. TARGU JIU JURIDICAL SCI. SERIES 89, 92-98 (2013).

[46]Silvia Lucia Cristea &Viorel Banulescu, *The Right to Personal Data Protection. The Right to Privacy.AComparativeLawApproach*,64ANALELE STIINTIFICEALE UNIVERSITATIIALEXANDRUIOANCUZADINIASISTIINTEJURIDICE1,03-09(2018).

[47]*Id.*

postulates a realm of privacy. Anartist finds reflection of thesoul ina creative endeavor. A writer expresses the outcome of a process of thought. A musician contemplates upon notes which musically lead to silence. Thesilence, which lies within, reflects on theabilityto choose how to convey thoughts and ideas or interact with others. These are crucial aspects of personhood. The freedoms under Article 19 can be fulfilled where the individual is entitled to decide upon his or her preferences. Read in conjunction with Article 21, liberty enables the individual to have a choice of preferences on various facets of life including what and how one will eat, the way one will dress, the faith one will espouse and a myriad other matters on which autonomy and self-determination require a choice to be made within the privacy of the mind. The constitutional right to the freedom of religion under Article 25 has implicit within it the ability to choose a faith and the freedomtoexpressornotexpressthosechoicestotheworld.Theseare some illustrations of the manner in which privacy facilitates freedom and is intrinsic to the exercise of liberty[48].

The excerpt represents the importance that has been accorded to right to privacy by the Supreme Court of India. Come what may, the future of interpretation of the data protection laws in India will be influenced by this landmark judgment for years to come. The sensitive personal data may only be transferred outside India for the purpose of processing…" the Bill notes, while adding that this doesn't apply to 'criticalpersonaldata'. Theinterpretationofrighttoprivacyinthespatial,functional andinstitutionalformshaslongbeenseenasaninhibitorofgenderequalityandthus has been subject to a lot of criticism from the feminist school of jurisprudence. The feminist school treats the right to privacy at home as an instrument to felicitate the subordination of women in their homes. This interpretation has been repeatedly attackedasaninstrumentforimmunizingthepowerimbalanceswithinthefamilies

[48]JusticeK.S.Puttaswamy(Retd.)andAnr.v.UnionofIndiaandOrs.,(2017)10SCC1

bytheexclusionsoftheconstitutionalschemeintheguiseofprivacy.Thespatialand functionalunderstandingoftherighttoprivacyhasbeenregardedasaninstrumentto "defend the exemption of marital rape from sexual assault laws, and to discourage state interference with domestic violence or child abuse.

The new Personal Data Protection Bill also contains three key clauses that were not previously included in the Srikrishna draft version and have raised some concern amongst technology companies and privacy experts. These include sections thatwill allow the Centre to ask any "data fiduciary or data processor" to hand over anonymised personal data or "other non-personal data" that will allow better governance or targeting of citizen welfare services.

Onthesurface,theproposed IndianDataProtectionActof2019 appearstoemulate new global standards, such as the right to be forgotten. Other requirements, like having to store sensitive data in systems that are located within the subcontinent, may put constraints on certain business practices and are considered more controversialbysome.Thedraftbillalsostatesthatthecentralgovernmentcanframe policy forthe digital economy with respect to non-personal data. Inparticular, it can direct any data processor to "provide any personal data anonymized or other non- personal data to enable better targeting of delivery of services or formulation of evidence-basedpoliciesbytheCentralGovernment". The final Bill slightly reverses India'sstand,notingthat"sensitivepersonaldatamaybetransferredoutside India", but should continue to be stored within the country. However, what remains to be seen is the legislative intent in enacting a strong data protection law.

Indiacouldexceedinglybenefitfromtheexperiencesofthecountriesthatareknown to have strong data protection regimes in place by avoiding the usual pitfalls. Given thefactthatIndia,alongwithworldismovingtowardsanincreasinglydigitalizedand globalized world, it becomes all the more important to address the issues of data protectionthatmayhavetrans-nationalaspectsattachedtothem.Inordertoputforth astrongcaseforaDataProtectionregimethatiscompatiblewiththeentitiessituated

abroad, and particularly in the developed world, the finder would deem it conducive to discuss the accepted principles of Data Protection in the developed world, particularly in the EU as well as the legislations in these jurisdictions.

1.5 Principles of Data Protection

RighttoPrivacy,asmentionedearlierisquiteanabstractandamorphousconceptand henceitisnorpossibletochalkoutadefiniteone-lineguidethatwouldleadthecourts to determine whether there has been an intrusion in the private domain of an individual[49]. Hence, numerous principles governing the right to privacy have been developed by the legislatures and courts all over the world to serve as the guide to effectiveadjudicationagainsttheclaimsofbreachoftherighttoprivacy.Someofthe notableprinciplesaretheOECDPrinciples[50],theUSConsumerBillofrightsandthe GDPR[51].However, a one size fits all strategy can not serve the purpose of effective legislationandhenceIndia,insteadofadoptinganyoftheseprinciplesshadtodevelop its own national privacy principles that would be suited to the Indian Constitutional values while borrowing the best practices from all over the world.

These principles must be aimed at securing the safety of the entire process of collection, storage, processing, access, retention and disclosure of information that canbeusedtoidentifyaparticularindividual.Inpursuanceoftheobjectivetodevelop NationalPrivacyPrinciples,thePlanning Commissionappointedacommitteeledby theJusticeAPShahto formulatetheprinciplesthatwouldgoon toform thecruxof the upcoming data protection legislation in India[52]. In 2012, a Group of Experts on Privacywasconstituted by theerstwhilePlanningCommissionunderthe

[49]DAVIDBENDER,COMPUTERLAW:AGUIDETOCYBERLAWANDDATAPRIVACYLAW,388-389(1ST ED.1978).

[50] OECD, _OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.

[51]AGupta,*SummaryOfTheReportOnPrivacyLawByTheGroupOfExpertsHeadedByJustice A.P. Shah*.MEDIUM.(July, 2019) ,: <https://iltb.net/summary-of-the-report-on-privacy-law-by-the-group-of-e xperts-headed-by-justice-a-p-shah-6e5917ea9c18> [Accessed 28 May 2020]

[52]SupraNote48at402.

Chairmanship of Justice AP Shah (Justice AP Shah Committee). The report of the Justice AP Shah Committee recommended a detailed framework that serves as the conceptualfoundationforaprivacylawinIndia,consideringmultipledimensionsof privacy. After a detailed deliberative and consultative exercise, it proposed a set of nine National Privacy Principles to be followed, broadly derived from the OECD Guidelines.[53]Thefinderwoulddiscussthesepprinciplesinanutshelltolocatethe Indianized jurisprudence of the data protection law through the principles identified by AP Shah Committee.

Notice: The first and perhaps the most important of the principles identified by the committee is the requirement of the notice to the data owner[54]. The principle highlightstheconceptofthedataownershipandmandatesthateveryprocessorofthe personal data of the individual shall give sufficient notice to the owner of the data. The notice must be couched in language that is easily understandable and sufficient to inform the data principal about the processing. The notice should further disclose the facts relating to the type of data which is being collected, the purpose for which suchcollectionisbeing made,thesecuritymeasuresthatthecollectorhas inplaceto ensure the security of the collected data[55]. The principle also mandates that the data principalshallbefromtimetotimebeinformedaboutthechangesmadeintheprivacy policy of the process and in case of any breach, immediate notice must be sent[56].

Consent: The second principle provides that the obtaining of the consent is a necessarypre-conditiontotheprocessingofthepersonaldataoftheindividuals. The processormaydenytheservicesincasetheconsentisrefused.However,whenthe

[53]WHITEPAPEROFTHECOMMITTEEOFEXPERTSONADATAPROTECTIONFRAMEWORKFORINDIA https://Www.Meity.Gov.In/Writereaddata/Files/White_Paper_On_Data_Protection_In_India_171127_Final_V2.Pdf

[54]ReportoftheJusticeAPShahCommittee,5(October16,2012).

[55]SupraNote48at403.

[56]SupraNote48at405.

processing is sanctioned by law and is in conformity with the other data protection principles, then the information collected by the agencies shall be anonymized[57].

CollectionLimitationPrinciple: Thedatashallbecollectedonlytotheextentwhich isabsolutelynecessaryforthefulfilmentoftheobjectiveforwhichthedatahadbeen collected[58].

PurposeLimitationPrinciple: Datacanbeprocessedonlyforthepurposesthathad beennotifiedtothedataprincipalatthetimeofobtaininghisconsent.Forprocessing data for any other purposes, a fresh consent has to be taken through notice[59].

1.6 The Foundations of Data Protection Regime in India

TheBNSriKrishnaCommitteehadlaidthefoundationofthebeginningofaneraof the establishment of a comprehensive code on the data protection regime in India[60]. The Narendra Modi government 2020 appointed a committee under the chairmanship of Justice (Retd.) B.N Srikrishna, which has been tasked with the mandate of proposing measures to effectively address issues around data protection and privacy. This committee has also been playing with the idea of a regulator, possiblymodelledonexistingregulatorybodieslikeTheSecuritiesandExchange

Board of India or the Reserve Bank of India.The lacunas in the existing laws relating to the absence of incorporation of the key data protection principles and the needtohaveamoreextensiveanddataprincipalcentriclawhadledtotheformation ofthecommitteetosuggesttheroadmapforanewandcomprehensivedataprotection

[57] SupraNote48at406.

[58] *Id.*

[59] *Id.*

[60] *JusticeSrikrishnaCommitteeSubmitsReportOn DataProtection.Here'reIts Top10 Suggestions*, The Economic Times. <https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms?from=mdr>

legislation. The 10-member committee led by Honorable Justice B N Sri Krishna; a former judge of the Supreme Court of India submitted its report containing the recommendations for a comprehensive data protection regime in India along with a draft data protection bill[61]. The recommendations mirrored the provisions of the GDPR(General data protection regime) to a great extent and provided for the adoption of the key data protection principlesintheIndianlegalarena[62].Atthetimeofitsrelease,thedraftbillhadbeen hailedasthefoundationofthecoreprinciplesoftheupcomingdataprotectionregime inIndia[63].Abriefanalysisofthekeyaspectsandrecommendationsofthecommittee reportshallbehandyinpavingthewayfortheanalysisoftheproposeddataprotection law in India.

The draft bill had defined the key aspects of data protection regime including the meaningofdata[64],processing[65],thepersonaldata[66],sensitivedata[67]etc.muchonthe linesoftheGDPR(General Data Protection Regime).Thenitprovidedrestrictedgroundsonwhichthepersonaldataof theindividualsmaybeprocessedbythestateandthecorporations[68].Thebillhadalso pitchedforstringentdatalocalizationnormswhileprovidingthatatleastonecopyof thedatasoughttobetransferredacrossthebordershastobestoredinIndia.Thedraft bill had also pitched for a broad meaning of the rights of the data principal and recognized, the right to data portability, the right to be forgotten[69], the right to accessibility[70]andtherighttocorrection[71].Further,thedraftbillhadlaidagreatdeal

[61] *Id.*

[62] Meity.gov.in.2020.*WHITEPAPEROFTHECOMMITTEEOFEXPERTSONADATA PROTECTION FRAMEWORK FOR INDIA*. <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf>

[63] *Id.*

[64] Sec.12PersonalDraftDataProtectionBill 2019.

[65] Sec.29PersonalDraftDataProtectionBill 2019.

[66] Sec.32PersonalDraftDataProtectionBill 2019.

[67] Sec.35PersonalDraftDataProtectionBill 2019.

[68] Sec.40PersonalDraftDataProtectionBill 2019.

[69] Sec.27PersonalDraftDataProtectionBill 2019.

[70] Sec.24PersonalDraftDataProtectionBill 2019.

[71] Sec.25PersonalDraftDataProtectionBill 2019.

ofemphasisontheimportanceofinformedconsent[72].However,oneofthesubstantial omissionsofthedraftbillwasthenon-inclusionoftherighttoerasureandnomention of the need to reform the surveillance regime in the country.

However, one of the most laudable aspects of the bill was the conception of an independent data protection authority that would be selected by a committee comprisingoftheChiefJusticeofIndia[73].Eventhen,whiletheSrikrishnacommittee suggested inclusion of the Chief Justice of India or his nominee and one expert of repute in the Selection Committee, the PDP Bill introduced in parliament provides for a committee comprising entirely of members from the executive, i.e. secretaries from departments of the Central government, without a judicial member and an expert. The power and discretion to remove any member of the DPAare vestedwith the Central government without a method or procedure for such removal being explicitly prescribed.[74] The protection of the salary of the members has also been diluted and it shall now be prescribed by the Central government. The Data ProtectionofIndia,asenvisagedbythedraftbillwouldhaveawiderangeofpowers including that of search and seizure and imposing heavy penalties.

The Committee's report was subjected to a lot of criticisms, ranging from having pushedtheneedtoprotecttheinformationalprivacyofthecitizensatabackseatwhile giving primacy to the economic aspects of the personal data.[75] It also drew ire from the academicians and right to information activists for its flawed composition. The members of the committee consisted of the personalities that had been vocal in support of the Aadhar Act and had even at various point of times, opposed the recognitionoftherighttoprivacyasafundamentalright.[76]Thereport,whilehaving

[72]Sec.02PersonalDraftDataProtectionBill 2019.

[73]Sec.02PersonalDraftDataProtectionBill,2019.

[74]WhyIndia'sProposedDataProtectionAuthorityNeedsConstitutionalEntrenchment,TheWire (2021), https://thewire.in/tech/india-data-protection-authority-needs-constitutional-entrenchment (last visited Feb 24, 2021).

[75]Id.

[76] The Data Protection Bill only weakens user rights, The Hindu (2021), https://www.thehindu.com/opinion/lead/the-data-protection-bill-only-weakens-user-rights/article30405339.

mirroredalotofprovisionsonthelinesofGDPRpromisedthedawnofahealthyand robust data protection regime in the country, failed to answer some of the pressing questions related to the safeguards against the intrusions of the state in the realm of the private affairs of the citizens.

The most significant deviation of the report can be traced in the philosophical overtonesofthereportthatseektoemphasizemoreontheneedofarobusteconomy instead of safeguards against the breach of the fundamental right to privacy. The report also, to a great degree misinterprets the landmark decision in the case of K S Puttaswamyv.UnionofIndia[77]ofIndiawhileignoringtheimportanceofthedoctrine ofproportionalityandhencepushesthefundamentalrightoverthebackseat.Someof theothercountsonwhichthedraftbillcameunderseverecriticismincludethefailure to recognize the ownership of data, the lack of provisions regarding notice of the breach, non-mentioning of the reforms in Aadhar etc.

India has come a long way from the days when the concept of data protection as confinedtothenarrowwallsoftheInformationTechnologyIndustries.Asnoted,the use of data has become an indispensable aspect of the Indian economy and hence there is need of a comprehensive framework that would cater the needs of data protectioninIndia.Inthefollowingchapter,thefinderwoulddiscusssomeofthe globally accepted principles of data protection in order to get a better understanding of the normative aspects of data protection legislation.

[77](2017)10SCC 01

CHAPTER2:GLOBAL INSTITUTIONS AND THEIR DATA PROTECTION PRINCIPLES

2.1 Introduction

InthepreviousChapterthefinderhasdealtwithsomeofthemostnotableaspects of the era of digitalization that have led to the privacy concerns all over the world. ThediscussionhasprovidedatheoreticalinsightintothePrinciplesofDataProtection but as the famous proverb goes, "*the taste of pudding lies in the eating*" it would be optimum to takeup a detailed study of the manner in which the provisions related to the concept of Data Protection in order to have a firm grasp on the practical aspects ofaComprehensiveDataProtectionCode.Thestudyalsobecomesimportantinorder to formulate a code that would be in synergy with the International Best Practices with regards to data protection.

It has been rightly opined by the academicians and the jurists all over the world that dataprotectioncannotbeachieved byacountryinisolation[78].Giventhefact thatthe source, storage and medium of transmission of the major chunk of data all over the world is the Internet, the numerous challenges faced by the regulators in affording a robust data protection regime cannot be met adequately at the national level[79]. The data knows no boundaries and hence there needs to be a trans-national framework aimed at securing adequate safeguards to the personal data of the citizens while ensuring an unrestricted cross-border transmission of data.

Inordertoeffectuatethepolicyoffreeflowofdataacrossthebordersand guarantee aprescribedthresholdofsecuritymeasures,thereneedstobeamutuallyagreed

[78]Frederik Zuiderveen Borgesius, Jonathan Gray &Mireille Van Eechoud, *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 Berkeley Tech. L.J. 2073 (2015).
[79]GUTWIRTH, S. ANDDEHERT, P., REGULATINGPROFILINGINA DEMOCRATICCONSTITUTIONALSTATE. IN PROFILING THE EUROPEAN CITIZEN 271 (2008).

framework on which the nations ought to base their data protection legislations[80]. Universally accepted principles of data protections can be instrumental in bringing uniformity and consistency in the data protection laws all over the world[81]. As we have witnessed in the previous chapter, the whole subject of data protection is quite abstract in natureand therecannot beaonesizesuit all formulathatwould servethe purpose of data protection.

Thisgivesrisetotheneedforhavingasetofprinciplesattheinternational levelthat would serve as a guide for the nations in framing their own data protection laws. Keeping this view in mind, numerous International and regional organizations have agreed upon some of the core principles that should be incorporated in the data protectionlawsofthecountries.[82]Thefinderwouldprimarilyfocusupontwoof the most important organizations that hold a great deal of influence over the data protection regimes all over the world.

2.2 UnitedNation'sDataProtectionPrinciples

The United Nations Personal Data Protection principles lay down the blueprint for a healthy data protection regime all over the world. While, most of the data protection enactmentsintheworlddovouchtoadheretotheseprinciples,minordeviationsfrom theseprinciplesarealsocommon.Importhereisthepersuasivevalueoftheprinciples recognized by the United Nations that act as a guiding principle for the states that genuinelylookforwardtocreatingarobustdataprotectionregimeintheir country[83]. WhiletheseprinciplesaresupposedtoguidetheUnitedNationSystemOrganizations incarryingouttheirmandatedwork,thepersuasivevalueoftheseprinciplesinglobal realmremainstobeenormous[84].TheGDPR(General data protection regime)andPersonalDataProtectionBill2019

[80]SupraNote73at274.

[81]SupraNote73at277.

[82]AlLutz,DiscussionPaper:DataProtection,PrivacyandSecurityforHumanitarianandDevelopment Programs

[83]*Id.*

[84]Will Thomas DeVries,*ProtectingPrivacyintheDigital Age*,18 BERKELEYTECHNOLOGYLAWJOURNAL 283, 311 (2003)

and numerous data protection legislations across the globe have these principles as thecornerstoneoftheirdataprotection regime[85].Theseprinciples (the "Principles") set out a basic framework for the processing of "personal data", which is defined as information relating to an identified or identifiable natural person ("data subject"), by, or on behalf of, the United Nations System Organizations in carrying out their mandated
activities.

FAIRANDLEGITIMATEPROCESSINGPRINCIPLE

The United Nations System Organizations should process personal data in a fair manner, in accordance with their mandates and governing instruments and on the basis of any of the following:

(i) theconsentof thedata subject;
(ii) thebestinterestsofthedatasubject,consistentwiththemandatesofthe United Nations System Organization concerned;
(iii) themandatesandgoverninginstrumentsoftheUnitedNationsSystemOrganizatio n concerned; or
(iv) anyotherlegalbasisspecificallyidentifiedbytheUnitedNationsSystem Organization concerned.

PURPOSE SPECIFICATION

Personal data should be processed for specified purposes, which are consistent with the mandates of the United Nations System Organization concerned and take into accountthebalancingofrelevantrights,freedomsandinterests.Personaldatashould not be processed in ways that are incompatible with such purposes.

PROPORTIONALITYAND NECESSITY

The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

[85] *Id.*

TRANSPARENCY

Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.

Among other prominent principles include the Accountability Principle which prescribes that United Nations System Organizations should have adequate policies and mechanisms in place to adhere to these Principles. Further the Data Protection Principles are hinged around a notion that in carrying out its mandated activities, a United Nations System Organization may transfer personal data to a third party, provided that, under the circumstances, the United Nations System Organization satisfiesitselfthatthethirdparty affordsappropriateprotectionforthepersonal data.

[86]ROSEMARYJAY,ANGUSHAMILTON,DATAPROTECTIONLAWANDPRACTICE445(1995).

International cooperation of civil and political rights from here on words referred as ICCPR

forbidden,unlessitisdoneinaccordancewiththelawfulprocedure.AnIndividualhas therighttoknowthereasonforwhichtheirdataisbeingused,thelocationwhereitis kept,theperiodforwhichitwasgathered,theabilitytogetitrectified,andsoon.This has also beenhighlighted throughout the comment.

The Human Rights Committee has time and again emphasized on the importance of lawful collection and processing of personal records. It has stated that "gathering and holding of personal information on servers, databases, and other devices, whether by public institutions or private persons or entities, should becontrolled by law." Althoughthecomment'simplicationsseemtoencompassthedigitalrealmoftheright toprivacy,therearesignificantgapsthatmustbefilled.Comment16shouldtakeinto account a larger perspective of the Right to informational privacy, as well as include anindividual-centricconceptofprivacy.TheECHR(European Convention on Human Rights)precedentswillbeveryusefulto countries in upgrading comment 16 to specifically hold the routine procedure of collectingpublicdata,agroundforthebreachoftherighttoprivacy.Thiswillprovide the basis for addressing the threat of mass surveillance and also broadening the reach of the provision to include the digital sphere in order to acknowledge all the possible threats faced by technical advancements.

Getting Rid of the 4th Amendment's based-Right to Privacy

The language of Article 17 of the ICCPR specifically references the expression "home,"givingtheimpressionthattheconceptofprivacyintheconventionislimited to "spatial privacy," that is, the privacy of personal spaces only. This means that the covenant's security will be limited to "protection from encroachment of man's own castle."However,inthisage,wherethepossibilityofinvasionofprivatepropertyhas switchedtoonlinemediums,suchasuccinctreadingoftheword"Home"wouldhave disastrous consequences.[87] Hence, the new clause should include "online private spaces"whichencompassesTwitter&Facebookpages,emails,andothersocialmedia accounts of an individual.

[87] Ibid.

Intheonlinerealmasoftoday,thesocialmediapagesandmobilephonesarethesole means by which an individual designates their identity in the public community. Electronic gadgets and social media profiles have largely displaced the century old definitionofprivatespace.[88]Article17shouldexplicitlyacknowledgethischange.For a long time, the courts of the member countries have interpreted the word "home" broadly,holdingittoinclude"placeinwhichprivatelifecanevolvefreely."Inorder torespecttheadvancementofprivatelifeinthemodernage,theconventionmustgrant theword"privatedomain"thebroadestpossiblesense,includinganymeansbywhich one can enter the online sphere.

Incorporation of Meta data in to the Definition of Correspondence

The meaning of the expression "Correspondence" is another necessary aspect of Article 17 of the convention that has been constricted. Although correspondences relating to telephone calls, letters, online communications, and other forms of communication have already been included in comment 16, the latest risks posed to personal data by "metadata" must be included in the framework of Article 17. The metadataareessentially separatecollectionsofinformationaboutpeople,andmaybe combined for statistical analysis and information collection. The degree to which the metadata can be used for identification and mass monitoring has been questioned by courts all around the world. The Supreme Court of India struck down a portion of Section 57 of the Aadhar Act for violating the rules of storage and putting intentional restriction, but the court failed to consider the disadvantages of metadata storage. Consequently, this would enablethe Indiangovernment to storeand process personal data of individuals through Aadhar, which is a legitimate portal.[89] The incorporation ofmetadataintheconceptof"correspondence"hasarisenasarequirementtoprevent suchirresponsibleignoranceoftheriskthatmetadatacanposetotherighttoprivacy.

Itmustberememberedthatmetadatahasimmensepotentialforbeingexploitedbythe governmentforsecuritypurposes.Withtheaidof m e t a d a t a ,otherinformation

[88] Ibid.
[89] Ibid.

regardingone'sfoodpatterns,places,andbehavioralpatterncanbereadilyaccessed, and it is thus important to put metadata into the framework of Article 17 of the convention.[90] This will undoubtedly extend the reach of the provision, making it crucial in combating the problem of mass metadata monitoring.

"When collected and examined, communications metadata can build a profile of an individual's life, including medical issues, political and religious views, alliances, relationships, and interests, revealing as much information as, or even greater detail thatmaynotbedistinguishablefromthecontentofcommunications,"wrotetheUnited Nations Special Rapporteur on freedom of speech.

It is worth noting that European courts and the judiciaries of other countries with advanced data protection regimes have also taken steps to hold that data related to internet use falls under the definition of "correspondence" as under Article 8 of the ECHR. Meanwhile, since metadata is not explicitly included in the analysis of communications, states have a large window to conduct mass surveillance and profiling. The accumulation of metadata over time will have significant ramifications on individuals' right to privacy all over the world.

2.3 Decoding the Unlawfulness of the Interferences with the Right to Informational Privacy

Threatstotheinformationalprivacyofthecitizensduetoincreaseddigitalizationhas emergedasaglobalissue.Thecorebusinessmodelofmanytechfirmsismonetizing thedatatheycollectfromusers—notonlyforthemselvesbutalsoforsellingtoothers. Not everyone is a privacy hawk, and millennials less so than earlier generations. However,aftertheinfamousCambridgeAnalyticaDataleaks,theawarenessrelating to informational privacy has grown considerably. In 2014, Cambridge Analytica, alongwithNixandSCLElections,becamecognizantofresearchworkatthe

[90]JordanJ.Paust,CanYouHearMeNow?PrivateCommunications,NationalSecurityandtheHuman Rights Disconnect, 15(2) Chicago Journal of International Law 612, 625 (2015).

PsychometricsCentreatCambridgeUniversity.TheresearchrevealedthatFacebook users'accountdatawhichispubliclyavailablecanbeutilizedtopreciselyestimatea user's personality traits according to the "OCEAN" scale, a psychometric model. Finderscreatedanalgorithmthatcouldpredictanindividual'spersonalitybased on the individual's 'likes' of public Facebook pages.

The algorithm and the consequent data harvesting to train the company's model eventually led to Cambridge Analytica helping political campaigns like 2016 US elections, Brexit and led the way to a worldwide scandal. After the data harvesting was exposed, it tarnished Facebook's image along with multiple penalties for data mismanagement.

After theFacebook/Cambridge Analytica scandalit became apparent with time that despiteallthegovernmenthearings,itrequiresspecialeffortsandinitiativesfromthe public to make technology companies realize it's high time they made genuine amends. When the European Union passed the GDPR, it was more about regulating thewaypersonaldatacouldbeusedthesecompanies.Itwouldstillnotallowusersto entirely stop how someone could collect their personal data.

WhatsApp -Facebook Privacy Policy Update

Withthegrowthofsocialmediausersallacrosstheworld,thethreatofinfringement ofinformationalprivacyhasbecomemoreapparent.Indiawhichisahotbedofsocial media users does lack a comprehensive Data Protection legislation and thus the risk ofunlawfulinterferenceintheprivacyofthesocialmediausersbecomesallthemore real. One of such threats have materialized in the form of the stark opposition to the newly changes Privacy Policy of WhatsApp. In a move that has garnered a lot of media attention as well as the backlash from the users, the social media platform changes its privacy policy. As per the new terms, the platform will share the data of their users with its parent company, Facebook.The government is examining and evaluatingtherecentprivacypolicyupdateannouncedbyWhatsApp,amidanoutcry over the controversial changes linking data of WhatsApp users to Facebook's other productsandservices accordingtosources.Itisapparentthatonlyonaccountofthe

regulatoryvacuuminIndia,theIndianusersofWhatsApparebeingtreatedassecond class citizens and their personal data/information is being commercialized by WhatsApp without providing a clear, specific and unambiguous notice to the users before obtaining their consent.

On the other hand, on account of the existence of a robust regulatory regime in Europe, WhatsApp is unable to do the same for WhatsApp users in the European region,whoseprivacyrightscontinuetoremainprotected.Thisaspectofthepractice of the company amply reflects the need of having a strict regulatory mechanism for ensuring Data Protection. In a move that goes blatantly against the principles of informational self-determination, the update in the policy has mandated the users to accept the new policy, failing which they'd lose the access to their chats.

Moreover, the concerns of the breach of privacy are not related only to the chats. Atmanirbhar Digital India Foundation (ADIF) a newly formed industry association of Indian startups, has alleged that WhatsApp's recent privacy policy update is a looming threat to the payments and financial data of users and has sought greater oversight from the authorities. The policy could also lead to increased data sharing between WhatsApp Payments and parent entity Facebook despite the instant messaging platform's position that the update applies only to WhatsApp Chat.

The public backlash has forced the company to postpone the implementation of the new policy for few months, however, absent any regulation there is nothing in law thatwouldinvalidatethisactionofthecompany.Oneofthepositivetakeawaysfrom the incident is the fact that the Indian public, in general has become more conscious about their Informational privacy. This may be evidenced by the shift of the users from the platform to other platforms and a steep decline in the user growth of the platform since the announcement of the new policy.

GDPR and Informational Privacy

The Article 17 of GDPR that postulates, "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawfulattacksonhishonorandreputation*[91]"seekstoprotecttheindividualsfrom the arbitrary and unlawful interference in their private life. While the General comment16expresslystatesthateventhelawfulinterferencesfromthestatethatare not in consonance with the principles laid down in the covenant shall be deemed to be unlawful. The fact that "lawful" interferences with the right to privacy is allowed under the convention, it becomes pertinent to afford adequate emphasis to the parameter to adjudge the lawfulness of the act through which the privacy of an individual is sought to be infringed[92].

Instrictsense,lawfulnessisapseudonymforthedomesticlawandeverylawthathas been validly enacted by the competent authorities of a state would fall within the scopeoflawfulinterference[93].However,theGeneralComment16expresslyprovides that such interference shouldn't be arbitrary and should be consistent with the provisions of the convention[94]. While, this observation of the committee is commendable, one must note that these provisions are applicable only to the aspects of human life that have been identified to form a part of the right to privacy. Given thefactthatthecurrentdefinitionoftherighttoprivacywithintheconventionisquite restricted and outdated, the provisions that seek to protect "unlawful" infringements servelittlepurpose. The Committeehas endorsed thefact that just because thereis a law providing for the infringement of the right to privacy, it doesn't become lawful. In a way, the committee proposes the inclusion of the due process clause for warranting the breach of privacy of the individuals.

[91]SeeSupraNote110at704.

[92]Supranote240.

[93]*Id.*

[94]PETERMARGULIES,THENSAINTHEGLOBALPERSPECTIVE:SURVEILLANCE,HUMANRIGHTSAND INTERNATIONALCOUNTERTERRORISM,82FORDHAMLAWREVIEW2137(2014).

The Inter-Parliamentary Union and the United Nations (Office of the High Commissioner for Human Rights) Committee has taken considerable efforts to outline the parameters to assess the lawfulness of the law through which the privacy is sought to be infringed.[95] The committee has laid down four-pronged test in order to determine the legality of the means through which the privacy of the individual is sought to be curbed[96]:

1. The law must be publicly accessible, meaning thereby that there must not be any element of secrecy attached with the provisions that seek to infringe in the private domainoftheindividuals.Thistestwouldensurethattheindividualsareawareofthe law under which their privacy is being infringed.
2. The second test incorporates the purpose limitation principle along with the fairness principle and lays that the data can be processed only for the legitimate aims.
3. The third test provides that the underlying principle of certainty meaning whereby that thelawshould amply describe thenuances of interference. The lawought to lay down an objective criterion to determine the group of people whose privacy can be infringed, the objective that is sought to be achieved by such infringement, the detailedprocedureforauthorizationofsuchinfringementofprivacy.Thelawshould also put in clear terms the time limit for which such processing of data must be allowed and the procedure for storage and erasure of such information.
4. There must be sufficient safeguards in place to protect against the abuse of the process.

It may be inferred that the lawfulness of the processing is not just limited to the fact thatthelawofthelandmustsanctionthelawprovidingfortheinfringementofthe

[95]Ohchr.org (2021), https://www.ohchr.org/documents/publications/handbookparliamentarians.pdf

[96]LeeA.Bygrave, *DataProtectionPursuanttotheRighttoPrivacyinHumanRightsTreaties*, 6Int'lJ.L.&Info.Tech.247,253-259(1998).

privacy[97]. At the same time, it must be pointed out that the personal data protection bill does in no way comes even close to satisfying any of these tests[98].

Oneofthemostvitalaspectsofruleoflawisthecertaintyofthelaw.Theregulations providing for the infringement of the right to privacy can't be tangled into a web of secrecy. As per the principles enshrined in the ICCPR, the citizens must have knowledge about the regulations that provide for the data surveillance. In case of absence of publicized law providing for the collection and storage of acts of surveillance,thelawwouldfailthetestoflegality.Oneoftheotherimportantaspects ofthesurveillanceistherequirementofspecificityandprecisioninthelaw.Thelaw providing for surveillance must be precise and purpose specific.As per the Human Rights Committee, General Comment 16, (Twenty-third session, 1988),the law providing for surveillance must not be vague and the "*relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted*[99]."

2.3.1 Theneedforsufficientsafeguards

The rationale behind such assertion is that adequate publicity of the law shall make thecitizensofthelikelyconsequencesoftheiract.Thelaw,"*mustbeformulatedwith sufficientprecisiontoenableanindividualtoregulatehisorherconductaccordingly and it must be accessible to the public"*[100]. The lack of specificity and precision of the manner in which the surveillance is dine and the purposes for which it is being done can be detrimental to its legality in the international law[101]. There ought to be sufficient judicial oversight within the regulatory framework to ensure the transparencyandnon-arbitrarinessoftheentireprocess.Itissubmittedthatthelack

[97] Brian Gorlick,*Human Rights and Refugees: Enhancing Protection through International Human Rights Law*, 69 Nordic J. Int'l L. 117 (2000).
[98]*Id.*
[99]Rangushamilton, data protection law and practice 445 (1995).
[100]Id.
[101]SupraNote115at 2442.

ofsuchsafeguardswould eventuallypavetheway forunlawfulintrusions withinthe private realm of the citizens.

ThesubsequentresolutionsoftheUnitedNationshaverepeatedlyemphasizedonthe need of establish a mechanism providing for the effective mechanisms that would lead to a greater degree of transparency and promote accountability within the surveillance system of the state.

While,thesufficientsafeguardsarenecessarytoreduceandeliminatethepossibilities ofarbitraryinterferenceintherighttoprivacy,itisequallyimportanttohaveeffective redressalmechanismsinplace.Themodesoffilingthecomplaintagainstthebreaches of the rights guaranteed under Article 17 must be adequately publicized. There are few parameters that have been identified by the OHCHR in order to ensure that the mechanism has the essential features to redress the infringements in informational privacy[102]. The first requirement is that of the notice which is based on the premise thatitisthedutyofthestatetoensurethatthecitizensoughttobeinformedaboutthe nuances of the interference and the legal claim that the citizens have against the infringement[103]. This is followed by the need of a prompt, effective and impartial investigation into the alleged breaches by the state.

One of the most essential tests of every law that seeks to infringe the privacy of the individual, is the need for it being non-arbitrary and reasonable. The Human Rights Committee has time and again has advocated for that the need for the non-arbitrariness ofthelawstemsfromtherequirementofhavinglawsthatarestrictlyin consonance with the aims and objectives of the covenant.The requirement of non-arbitrariness adopts within its fold the elements of necessity, proportionality and legitimacy as well.In order to justify the intrusion into the right to privacy of the citizens,thestatemustinsimplestterms, *"demonstrateinspecificandindividualized*

[102]JordanJ.Paust,CanYouHearMeNow?PrivateCommunications,NationalSecurityandthe Human Rights Disconnect, 15(2) Chicago Journal of International Law 612, 625 (2015).
[103]*Id.*

fashion the precise nature of the threat and the necessity and proportionality of the specificactiontaken,inparticularbyestablishingadirectandimmediateconnection between the [restricted right] and the threat[104].” The signatory states have usually chosentoconstruethetextofArticle17inthemostliberaltermsandinferredittobe flexible enough to contain inherent limitations when it comes to the matters of national security and combating terrorism. It is a matter of common knowledge that thestatesdotendtousetheaspectsofnationalsecurityandpublicinterestasthemost common justification of infringing the right to privacy. While, there is a genuine concern regarding protection of the national security and combating terrorism, there isanecessitytosetforththelimitationsconcerningtheseissuestopreventthemfrom becoming an instrument for enabling mass surveillance.

2.4 African Union’s Data Protection Framework

The African Union (AU) was formed in 2002 to replace the Organisation of African Unity,consistsof55Africanstates,anditsbroadobjectivesincludeestablishingpeace andsecurity,andfosteringdevelopmentandsocio-economicintegrationontheAfrican continent. Cyber security, and especially cybercrime, is viewed as a growing concern in Africa. AnAfrican Union Convention on Cyber Security and Personal Data Protectionwasdraftedin 2011toestablisha‘credibleframeworkforcybersecurityin Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.’ The AU postponed the adoption of the Convention several times before finally adopting it in June 2014. It addresses three main areas:

(1) electronic transactions,

(2) personaldataprotection,

(3) cybersecurityand cybercrime.

The treaty will enter into force 30 days after the 15thinstrument of ratification or accessionisdeposited.AUmemberstatesalsohaveobligationsrelatingto

[104]Supranoteat250.

fundamentalfreedomsandhumanrights,assetoutindeclarationsandconventionsof theAUand theUnited Nations. This includes the commitment to respect, protect and promote the right to privacy, and personal data protection. In a number of instances, therighttoprivacyisalreadyestablishedinmemberstates'constitutions(forexample, Botswana, Democratic Republic of Congo, Egypt, Ghana, Kenya, Nigeria, Sierra Leone,SouthAfrica,Tanzania,Uganda,ZambiaandZimbabwerecognizetherightto individual privacy in their national constitutions as a fundamental human right). All thesepoliciesandobligationshaveimplicationsintermsofthesafe,transparent,robust and privacy-respecting exchange of personal data across borders and between jurisdictions. This, in turn, imposes a burden on AU member states to ensure that progress towards regional integration, free trade and development is not hindered or mademorerisky,byaninabilitytoexchangepersonaldatasecurely,reliablyandwith appropriate respect for individuals' rights. In parallel, safe, robust and privacy-respectinguseofpersonaldataisanessentialenablerofAUmemberstates' abilityto do the following:

- Maintaintheirownself-determinationintheinformationsociety,andkeep abreast of rapid change
- Capitalizeontechnologicalinnovation.
- Createandsustaintrust inadata-driven economy

Tosustaintrustinthedata-driveneconomy,AUmembersmustacknowledgetherole personal data plays, and the economic forces it generates. When successful, the data-driven economy can create economic growth, deliver compelling and innovative services, and improve the quality of life. However, the data-driven economy can also have a dark side, where personal data is handled in exploitative or abusive ways, and wheretheinterestsofthedatasubjectaredamaged.Thecostandriskinherentinthese casessometimesonlybecomesapparentwhen thingsgowrong—whenthereisadata breach,orfraudisexposed.Thiscanhaveaprofoundeffectontrustandconfidencein online services, and a corresponding impact on the data-driven economy. The Guidelines recommend steps to reduce the risk of these latter, unwelcome outcomes.

2.4.1 Personal Data Protection Aspects of the Convention

While, the convention deals extensively with the aspects relating to cybercrime and cyber security, the contours of data protection principles merit our attention for severalreasons.Theprincipleslaiddownintheconventionwillheraldthebeginning of a uniform cross border transaction of data amongst the member states while providing adequate protection to the rights of the citizens. The objective of the conventionprovidesthat"*EachStatePartyshallcommititselftoestablishingalegal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data*[105]." Further, the objective adds that such frameworks established by the states will afford adequate protectiontotherightsoftheconcernedcitizenswithrespecttoprocessingofpersonal data.Theconventionisquitewideinitsscopeanditprovidesthattheprovisionsshall be applicable to[106]

> *"Anycollection,processing,transmission,storageoruseofpersonaldataby anaturalperson,theState,localcommunities,andpublicorprivatecorporate bodies; b) Any automated or non-automated processing of data contained in or meant to be part of a file, with the exception of the processing defined in Article 9.2 of this Convention; c) Any processing of data undertaken in the territory of a State Party of the African Union; d) Any processing of data relating to public security, defense, research, criminal prosecution or State security,subjecttotheexceptionsdefinedbyspecificprovisionsofotherextant laws".*

The right to privacy encompasses, according to Harms J, "*the competence to determinethedestinyofprivatefacts*.[107]"Italsomeansthat"*theindividualconcerned*

[105] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Article 8(1).

[106] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Article 9(1).

[107] NMvSmith(FreedomofExpressionInstituteasAmicusCuriae)2007(5)SA250(CC).

is entitled to dictate the ambit of disclosure, for example a circle of friends, a professionaladviserorthepublic.[108]"Theindividualmayalsoprescribethepurpose andmethodofthedisclosure,andmaydecidewhenandunderwhatconditionsprivate facts may be made public.

In *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* the court further wentontoholdthattheassumptionthatothersareallowed accesstoprivatemedical information once it has left the hands of authorized physicians and other personnel involved in the facilitation of medical care is fundamentally flawed. It fails to take intoaccountanindividual'sdesiretocontrolinformationabouthimorherselfandto keep it confidential from others. In terms of the constitutional right to privacy, a personalso has theability to decidewhat information heorshewishes to discloseto the public.[109]

Thesecondnotableprincipleidentifiedundertheconventionisthefairnessprinciple which requires that the data ought to be processed for lawful purpose in a fair and a transparentmanner.[110]Theotherprinciplesexpresslyidentifiedundertheconvention are the principle of purpose limitation and the principle of storage limitation. It provides that the data shall be processed only up to the extent for which such processing is absolutely necessary and only for the purposes for which the data is collected. The principle of storage limitation warrants that the data shall be deleted after which the purpose for which they have been collected is fulfilled.

One aspect in which the convention has a broader scope that its counterpart legislations in India are the requirement of confidentiality in data processing where thesensitivedataoftheindividualsareinvolved[111].Theconventionlaysdownawide

[108]Id.

[109]Id.

[110] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Principle 5.

[111] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Article 14.

range of security measures to ensure that the data is processed with adequate transparency and security. Whereas, thedefinition ofsensitivedatais concerned, the convention adopts a very wholesome definition and unlike India, the processing of personal data is completely barred.The convention provides in express terms that the, *"State Parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject*[112]." Notethattheconventionwasadoptedwaybackin2014whenthecourtsinIndiawere yet to recognize the core traits of the individuals to be inherent part of the right to privacy. The rulings in *Navtej Singh Jauhar v. Union of India*[113] and *Joseph Shine v UnionofIndia*[114] thatrecognizedtherighttosexualprivacyandinterpretedtheright to privacy to be centered around the individual rather than the places or the society had already found a place in the provisions of the convention around half a decade ago. However, there are few exceptional cases wherein such sensitive data can be processedbuttheyhaveclearlybeenidentifiedandtheinclusionsofsuchexemptions are based by far on the doctrine of proportionality. The data which has already been made public by the data owner can be processed for the purpose for which such disclosure was made[115]. The other cases wherein such data can be processed are for journalistic and artistic purposes[116], for public welfare[117], for performance of contractual obligations.[118]

[112] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Article 14.
[113]NavtejSinghJauharv.UnionofIndia,(2014)5**SCC**438)
[114]JosephShinevUnionofIndia,(2019)3SCC 39
[115] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Article 13.
[116] African Union (AU) Convention on Cyber-security and Personal Data Protection (AU CCPDP), Article 14(3).
[117]*Id.*
[118]*Id.*

2.5 OECD(Organization of European Corporation and development)Principles on Data Protection

The OECD, Organization for Economic Co-operation is a global organization with over36countries.Basicideasaboutprivacyprotectionemergedinthe1970's,dating back to the advent of the "Information Society" and the introduction of computers into various areas of economic and social activity.[119] During this time period, there was a growing public perception that the greater need for information, and the proliferation of computerized systems, would result in a reduction in the power of individuals to control the personal information collected and stored about them. Computers were seen as a technology for processing large amounts of data quickly andcheaplyandasatechnologywhichconcentratedenormouspowerinthehandsof computer specialists and data processing managers. The combination of computer technologyandtelecommunicationswasalreadyholdingouttheprospectofcomplex information and communications networks at the national and international level.[120]

In the 1970's the Member Countries of the OECD reached a consensus on issues related to the protection of privacy to promote the free flow of information across their borders and to prevent legal issues related to the protection of privacy from creating obstacles to the development of their economic and social relations. To this end,theOECDCouncilonSeptember23,1980,adoptedthePrivacyGuidelines.The Guidelines were intended to form the basis of legislation in the organization's MembersStates.AtthecoreoftheGuidelinesisasetofeightprinciplestobeapplied to both the public and private sectors

Most of them have a comprehensive data protection code aimed at securing the greatestprotectiontotherighttoprivacyoftheindividuals.Itistobenotedthatmost oftheselegislationsarebased upontheprincipleslaiddown intheGuidelineson the

[119]Core Privacy Principles - The OECD Guidelines, Marcomm.mccarthy.ca (2021), https://marcomm.mccarthy.ca/pubs/share2.htm

[120]Core Privacy Principles - The OECD Guidelines, Marcomm.mccarthy.ca (2021), https://marcomm.mccarthy.ca/pubs/share2.htm

Protection of Privacy and Trans-boundary flow of data[121]. The guidelines framed by the members countries as back as in 1980 are considered to be the first step of the worldcommunityinchalkingoutcomprehensivedataprotectionprinciples[122].These earliest formulations of the right to privacy, to this day continue to be the backbone of every robust and effective data protection regime in the world.

The guidelines, as the name suggests are not binding on the member countries but havewielded great influenceoverthecountries in theAsia-pacificregion. However, with the adoption of the European Union Directive 108 the influence of the OCED guidelines started waning and in order to optimize the guidelines to suit the needs of the21st centuryprivacychallenges,theOCEDGuidelines2013wereadopted[123].The guidelines seek to achieve two-fold objective, the first of them being the need to ensure the free flow of data across the countries and the second being the need to provide necessary safeguards to the data.However, the regulations do provide that there can be legitimate restrictions on the free flow of the data.[124]

Following aresome of the most pertinent objectives that weresought to be achieved by the member states through these guidelines.

> "a) the need for generally continuous and uninterrupted flows of information between countries,
> b) the legitimate interests of countries in preventing transfers of data whicharedangeroustotheirsecurityorcontrarytotheirlawsonpublic order and decency or which violate the rights of their citizens,
> c) theeconomicvalueofinformationandtheimportanceofprotecting "data trade" by accepted rules of fair competition,

[121] Oecd.org. 2020.*G20/OECD Principles Of Corporate Governance- OECD,*: <https://www.oecd.org/corporate/principles-corporate-governance/>

[122] *Id.*

[123] *Id.*

[124] *Id.*

d) theneedsforsecuritysafeguardstominimizeviolationsof proprietary data and misuse of personal information, and

e) thesignificanceofacommitmentofcountriestoasetofcore principles for the protection of personal information[125]."

Prima facie analysis of the objects reflect that the initial efforts to lay down the principlesofdataprotectionwereaimedatobtainingeconomicviabilitythroughcross border transfer of data. The other objectives sought to be achieved by the guidelines felicitating the mutual understanding amongst the member countries to adopt the minimumstandardsofprotectionofdataand bringingagreaterdegreeofuniformity between the laws concerning data transfers among the countries[126] to make sure that undue interferences in the free flow of the data[127] while ensuring that the risks associated with such transfers are reduced to a bare minimum[128].

The guidelines are mere directional in nature and are not binding on the member states.Theseprincipleslaydownthebareminimumstandardsthatthememberstates shouldadopttofelicitatethefreeflowofdataand requisitesafeguards. Inpursuance ofthisobjective,thestateshavealsomutuallyagreedtosupplementtheseguidelines byadoptingnewmeasurestostrengthenthedataprotectionframeworkintheirstates and beyond the boundaries.

2.5.1 Collection Limitation Principle

Thefinderthinks it pertinent to discuss theprinciples emancipated in theOCED guidelines to trace the founding pillars of the modern data protection regime in the world.Itoughttobehighlightedatthisveryjuncturethattheseprinciplesnottobe

[125]Oecd.org.2020.*OECDGuidelinesonTheProtectionOfPrivacyAndTransborderFlowsOfPersonal Data - OECD.* [online] Available at: <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [Accessed 29 May 2020].

[126]Id.

[127]Id.

[128]Id.

read as discreet principles independent of each other as the data protection is an interconnectedsubjectandhenceitsprinciplescan'tbeconstruedinisolationtoeach other[129]and in a manner that gives widest amplitude to their interpretation.

The first principle laid down in the guidelines is the collection limitation principle that prescribes that the data collected should be limited. The principle is intended to inhibit the indiscriminate collection of data of the individuals and thus without spelling out the particulars, it merely lays down that there should be a limitation on the collection of data. It lays down that "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject[130]."

Theprinciplehas continuedtoactasaguidinglighthouseforthememberstatesand the countries all over the world to prescribe a cap on the collection of the personal data and further lay down the restrictions on which the data should be collected and thereafter processed. As may be noticed, the principle is couched in very general terms and the limitation prescribed in the principle is understood to be applicable to the amount of data collected, this implies that the data that is being collected should betheminimum,necessaryforachievingthepurposeforwhichitisbeing collected.

Theotheraspectsofthisprinciple prescribethatthedataprocessorsshouldobtainthe consent of the data principal before their data is collected. This principal is based on the fact that there is a need to curb the malicious practice of obtaining the personal data of the individuals without obtaining their consent.

[129]SupraNote115at 209.
[130]*Id.*

2.5.2 Data Quality Principle

Although couched in a positive language, the meaning of the Data quality principle has been interpreted as a limiting principle. It provides that the

> "*Personal data should be relevant to the purposes for which they are to be used, and,totheextentnecessaryforthosepurposes,shouldbeaccurate,completeand kept up-to-date*[131]".

The principle specifies that the data collected for a specific purpose should be sufficientforthepurposeforwhichitisbeingcollected.Thishastobeinterpretedas alimitationonthedatacontrollerstocollectonlythedatathatisessentialandrelevant for achieving the said purpose.

2.5.3 Purpose Specification Principle

The purpose specification principle provides that the purposes for which the data is being collected and sought to be processed must be specified and be informed to the data principal and any subsequent variations in the purpose must also be conveyed.

> *"Thepurposesforwhichpersonaldataarecollectedshouldbespecifiednot laterthanatthetimeofdatacollectionandthesubsequentuselimitedtothe fulfilmentofthosepurposesorsuchothersasarenotincompatiblewiththose purposes and as are specified on each occasion of change of purpose*[132]."

Theprincipleprovidesthatwhentheobjectiveforwhichthedatahadbeencollected, has been fulfilled then the said data must be destroyed.

[131]Tschentscher,A.,2017.PrivacyandDataProtectionbyRulesRatherthan Principles. *SSRN Electronic Journal*.
[132]*Id.*

2.5.4 Use Limitation Principle

Thisprincipleisaimedatpreventinganysortofunauthorizeduseofthedatacollected by the data controller. The principle provides that any deviations from the purposes for which the data had originally been collected would be deemed to be unlawful. Only with the consent of the data principal or with the authority of the law, such deviations may be allowed. For instance, it may be provided that data which have beencollectedforpurposesofadministrativedecision-makingmaybemadeavailable for research, statistics and social planning.

2.5.5 Security Safeguards Principle

Thesecuritysafeguards principleisaimedat effectuatingthesecondobjectiveofthe OCEDguidelines,thatistoaffordadequatesecuritytotheprocessedpersonaldataof the individual. The principle provides that:

> *Personaldatashouldbeprotectedbyreasonablesecuritysafeguardsagainst such risks as loss or unauthorized access, destruction, use, modification or disclosure of data*[133].

Theemergencesofconceptslikeprivacybydesignanddataanonymizationhavetheir genesis in this principle. Also, the other principles like the accountability and openness principles are intrinsically interconnected with the security safeguards principle.

2.5.6 Openness Principle

Theopennessprincipleorthetransparencyprincipleisaimedatsecuringthattheright of the data principal to access their data is given its true meaning. The principal prescribes that the data controllers should voluntarily take steps to keep the data principals informed about the purpose for which their data is being collected and in general the data principal must be kept in loop about the entire process.

[133] *Id.*

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller[134]."

Theprinciplemandatesthatallthisinformationmustbereadilyavailableandthedata principal should not face any difficulty in obtaining the information about the one who is processing their data, the purpose for which their data is being processed etc.

2.5.7 Individual Participation Principle

Theprincipleaffirmsthemostimportantaspectofeveryrobustdataprotectionregime allovertheworld.Theprincipalpitchesfortherightofthedataprincipalstohavean access to their data as a matter of routine and without any legal or technical hassles. Thedataprincipalbeingtheownerofthedatahasarighttoknowwhetheraparticular datacontrollerhasinformationrelatingtohimandtoobtainalltheinformationrelated to it. The principle provides that:

"Anindividualshouldhavethe right:

a) toobtainfromadatacontroller,orotherwise,confirmationof whether or not the data controller has data relating to him;

b) tohavecommunicatedtohim, datarelating tohim

1. *withina reasonabletime;*
2. *ata charge,if any, thatis not excessive;*
3. *inareasonablemanner;and*
4. *ina formthat is readilyintelligibleto him;*

[134] Oecd.org. 2020.*G20/OECD Principles of Corporate Governance- OECD*,: <https://www.oecd.org/corporate/principles-corporate-governance/>

c) tobegivenreasonsifarequestmadeundersubparagraphs(a)and
(b)is denied, and to beable to challengesuch denial; and
d) to challenge data relating to him and, if the challenge is successful
to have the data erased, rectified, completed or amended[135].”

The principle attaches a great degree of individual participation in the processing of dataandgoesontoprovidethatsuchrequestsonthepartofthedataprincipalsshould notberefusedandincasethedisseminationofsuchinformationisrefused,itmustbe subjectedtoanappellateauthority.Itissubmittedthattheprincipleformsthebedrock of the modern conceptualization of a robust data protection framework, at the centre of which lies the data principal.

Theobjectoftheprincipleistokeepthedataprincipalinloopaboutthepossibleuses towhichtheirdatacanbeput.Inordertogivetruemeaningtotheelementofconsent as a pre-condition to processing of personal data, it is absolutely necessary to keep the data principal informed about their data.

2.5.8 AccountabilityPrinciple

A data controller should be accountable for complying with measures which give effect to the principles stated above.

The accountability principle seeks to impose the liability upon the data controller in case they fail to comply with the measures required to be taken for adhering to the mandates of the principles. The principle is based on the normative aspect of the purpose of processing of data, as the data is processed forthe benefit of the one who processes the data and hence it is their responsibility to make sure that all steps are taken to protect the data.

[135] *Id.*

2.6 Dissertation

The Chapter essentially traces the foundations of the data protection regime while analyzing the several data protection principles recognized by the global institutions all overtheworld.Theundertaken study provides thefinder with an insight into thekeylimbsofarobustdataprotectionregimeinademocraticsociety.Withspecial emphasisontheOCEDPrinciples,thefinderseekstoformulateanoptimumdata protection model for the Indian scheme in the upcoming chapters. The study has enabled the finder to identify the key aspects of a robust data protection regime.

The discussions in the previous chapters have amply revolved around the jurisprudentialissuesrelatingtotheconceptofdataprotectionallovertheworld.Be thatasitmay,everysovereignnationhastherighttoadoptanapproachinitsnational legislation as perherneeds and thus itwould notbeout ofplaceto discuss about the Data Protection regime in some of the jurisdictions in order to examine the ways in which they have adopted the principles discussed in the previous chapters.

The Big Data imposes a great deal of measures to ensure data security of the individuals all over the world. With the advent of Internet of Things, the volume of dissimilation of data will become much more easier which will proportionally increase the risk of threat to individual data. An enormous amount of data that gets involved in the process is personal data and may include the personally identifiable information about the data subjects.

CHAPTER3:DATA PROTECTION IN EU,US AND UK

3.1 Introduction

Bigdataisallaboutthestrategicandchannelizeduseofdataforthepurposesforeign tothepurposeforwhichtheywerecollected.[136]Thismayinvolveprocessing,analysis and evaluation of data in order to provide customized services. For instance, the shopping pattern of individuals in a particular area may be processed to show the internetusersspecificadvertisements.Theprocessofcombinationandrevaluationof thesedatacanbeusedfor,financialtransactions,creditworthiness,medicaltreatment, private consumption, professional activity, tracking and routes taken, internet use, electronic cards and smartphones, video or communication monitoring[137].

No doubt, the scientific benefits of big data may be many but that doesn't mitigate the volume of risk attached to their handling. There are possibilities of manipulation of these data and the use of automotive information based on artificial intelligence further reduces the scope of human intervention. This implies that the right to object andotherimportantrightsrecognizedbythe well-developeddataprotectionregimes get nullified. The processing and evaluation of large volume of data thus have emerged as a new challenge to the data protection regime all over the world. The GDPRrecognizestheimpendingchallengesrelatedtothedataprotectionvisavisbig data[138].However,duetothelackofhumanintervention,alotofseriousissuesrelating totherightandtheremedieshavearisen.Inthenextsectionweshalldiscusssomeof theimpendingchallengesthatthebigdataissettoposetothedataprotectionregime. TheIndianbillmirrorsandappearstoendorsepartsofthestancetakenbytheGDPR. Federaldataprivacyapproaches intheUnitedStateshavetodatetakenamuchmore

[136]MatthiasBerberich,MalgorzataSteiner,*BlockchainTechnologyandtheGDPR-Howto Reconcile Privacy and Distributed Ledgers*, 2 EUR. DATA PROT. L. REV. 422, 431-432 (2016).

[137]STUARTRUSSELANDPETERNORVIG,ARTIFICIALINTELLIGENCE:AMODERN APPROACH, 122-124 (1ST ED. 2009)

[138]EuropeanCommission,'QuestionsandAnswers -Dataprotectionreform'(Pressrelease,21 December 2015) accessed 13 August 2019.

laissez-faire approach to data regulation than the approach embodied in the EU's GDPR.Thisperhapsreflectsafundamentallydifferentunderstanding ofhowhuman rights pertains to the protection of online speech and data privacy. The U.S. largely views the protection of online data and information as less the government's responsibility than, for example, many counterparts in the European Union.

What does the bill mean for India's role in the global data conversation? India is an important player in the global internet policy space.Indian government leadershipiseagerto position India as a global leader on democratic data regulation andhas

largelysucceeded.Indiahashighlevelsofglobalinternetpolicyparticipationthatis, activity in the UN General Assembly and elsewhere on internet issues and analysts have rated the nation high on its ability to influence international policy.

The specific design of institutional choices that India adopts for data protection is likelytohaveasignificantimpactonIndia'seconomy.Theseconsequencescouldbe direct (such as increased compliance costs) or indirect (the potential stifling of innovation,andoverallproductivitylosses).Whilethenumericalestimatesdiscussed may not necessarily hold true with respect to India, they do highlight the disparate ways in which a GDPR-style data protection law could impact certain sectors of the Indian economy.

Existing literature on the GDPR suggests significant economic consequences for the EU, with a potential to impact small and medium-sized enterprises (SMEs), labor markets, cross-bordertrade, and overall economic growth. A detailed analysis ofthe literature assessing the impact of the GDPR highlights both the potential negative consequences of a GDPR-like data protection law for India and the necessity of undertakingsimilarstudiesinIndiapriortothebill'simplementation.Asalegislative

proposal that will have a significant impact on critical sectors of India's economy, it isvitalthattheDPC'sproposedbillbecarefullyandcriticallyevaluatedincontextof the data protection regimes in the US and EU.

The right to personal data protection bears close resemblance to the right to respect for the private life. While both of these rights are based upon the theme that an individual havearighttolivetheirlifewithdignityandhence,theyneedapersonalspherewhich

is free from outside intrusion, the right to respect for private life is a much broader concept. It includes within itself the right to fundamental freedoms, the right to life etc. whereastherighttoprotectionofpersonaldataisanorganicconceptwhichencapsulates a mechanism that protects the personal information of the individuals by a systematic regulation for processing, storage and security of the data... Article 8 of the EU Charter ofFundamentalRights(theCharter)notonlyaffirmstherighttopersonaldataprotection, but also spells out the core values associated with this right. It provides that the processing of personal data must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law.

The right to protection of personal data is guaranteed to individuals every time their data is processed, irrespective of the fact that such processing has any impact on the privacyofthesubject[139].Although,suchprocessingmayinfringetherighttoprivacy but even in cases where such processing has no bearing on the right to privacy, the right to protection of data comes into play. The European court of justice has interpreted the term privacy in very broad sense and the instances where mere collection of the individual data has been held to be a potential to breach the right to privacy in case of unauthorized transmission to the third parties.

3.2 Role of ECHR In Developing Data Protection Jurisprudence In EU

The ECHR provides that, everyone has the right to respect for his or her private and family life, home and correspondence[140]. The theme of the European data protection regime revolves around restricting the interference of the public authority in the private sphere of life of the individuals. Other than the cases involving legitimate publicintereststherighttobeleftaloneisrecognizedasabasictenetofdignity-based life. With the emergence of revolutionary technological changes, the meaning of the term right to be left alone assumed a much wider definition as the states recognized theincreasingthreatofbreachofprivacytherebygivingapushtoevolutionof

[139] See CJEU, Joined cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, Opinion of Advocate General Sharpston, 17 June 2010, para. 71

[140]See,GaskinvUnitedKingdom(1989)12EHRR 36,

conceptslikeinformationalself-determination.[141]Thegrowingneedofregulatingthe personaldatasawalargenumberofstatescomingupwithlegislationsregulatingthe processing and storage of personal data of the citizens in early 1970‘s.

TheEuropeancourtshavetakenaverystrictstanceontheissueofprotectionofdata andhavegivenaveryliberalinterpretationoftherighttoprivacyandhavedescribed, ascoveringintimatesituations,sensitiveorconfidentialinformation,informationthat could prejudice the perception of the public against an individual, and even aspects of one‘s professional life and public behavior. It can inferred that the such wide interpretationofthetermprivacyisintendedat fillingallthepossiblepotholesinthe interpretation that may have the potential to jeopardize the right to privacy of the individuals.

In Digital Rights Ireland[142], the CJEU while examining the validity of Directive 2006/24/EC on the issues concerning the fundamental rights to personal data protectionandrespectforprivatelifeheldthatthedirectivewasindirectlyinterfering with the right to privacy of the individuals while observing that:

> *“When taken as a whole, the personal data retained pursuant to the directive, which could be accessed by competent authorities, could allow “very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanentortemporaryplacesofresidence,dailyorothermovements,the activities carried out, the social relationships of those persons and the social environments frequented by them.”*

Oneof the key aspects of any healthy Data Protection Regime is the scope of Rights thatitrecognizesforthe citizens.An expressrecognitionofsomeoftherights which

[141]GGFUSTER,EMERGENCEOFPERSONALDATAASAFUNDAMENTALRIGHTINTHEEU,106-113 (1ST ED. 2014).
[142]SupraNote168at 115.

areunderstood to bethe contours oftheRight to Privacy is an essentially element of arobustDataprotectionregimethatseekstoupholdthesanctityofallcherishedright in all its forms. Therefore, it is deemed optimum to analyse some of the key rights recognized by the EU law in the field.

3.2.1 Right to Religion

Inthepresenttimes,one'sfaith,beliefandmethodofworshipmayhaveahugeimpact onthewaytherestofthesocietyviewsthemandhencetheprotectionofdatarelating to religious belief is considered an important facet of right to privacy. Anyone's personalreligious,spiritualorphilosophicaldataisconsideredassensitivedataunder theEUCharteroffundamentalrights.Article9ofthecharterprotectsthefreedomof theindividualstothought,religionandconscienceandanybreachofdataconcerning these rights are presumed to threaten these rights.[143]*In Sinak Isik v. Turkey*[144], the petitionerhadchallengedalegislationonthegroundofwrongnameofthereligionin the identity card. Holding the directive as illegal, the ECtHR noted that,

> *"Religious freedom entails the freedom to manifest a person's religion in community with others, in public and within the circle of persons sharing the same faith, but also alone and in private. The domestic legislation applicable at the time obliged individuals to carry an identity card, a document that had to be shown at the request of any public authority or private enterprises, indicating their religion. Such obligation failed to recognize that the right to manifest one's religion also conferred the reverse, i.e. the right not to be obliged to disclose one's beliefs."*

Notably,thegovernmenthadarguedthattheobligationtomentionthereligioninthe identity card had been dropped and those who chose not to mention their religion couldoptfor leavingitblank.Theargumentwasrejected bythecourt ontheground

[143]SeeEUROPEANUNIONAGENCYFORFUNDAMENTALRIGHTS, HANDBOOKONEUROPEANNON-DISCRIMINATION LAW29-30 (1STED., 2011).
[144]ECtHR,SinanIşıkv.Turkey,No.21924/05,2February2010.

that such recusal would put the concerned individuals in an odd position and hence the contested legislation was declared to be violative of the Article 9 of the ECHR. Some commentators argue that the Churches that maintain the records of the information about their visitors must have been mandated by the Article 91 of the GDPR to form internal regulations for data processing which must comply with the norms of GDPR.[145]

3.2.2 Financial Interests

The advent of digital era has brought a paradigm shift in the way business is done throughout the world. The importance of data had never been so highlighted and deservingly so, a lot of economists agree that the data is the new oil. A lot business aroundtheworldhavedataprocessingasafocalbusinesselementandapprehensions are raised time and again about the economic implications of strict compliance measures for protection of personal data by both the data controllers and the data subject.Thequestionastowhetherthefinancialinterestscanbetreatedasajustifiable groundforlimitingtheprocessofdatawasraisedinthelandmarkGoogleSpaincase. Thecourtheldthatthedataaccumulatedbythesearchenginesdohaveapotentialto cause serious privacy threats in the wake of vast amount of personally identifiable information held by them.[146] While addressing the argument about the underlying economicinterestinsuchprocessingofdata,thecourtheldthat,afairbalanceshould besoughtinparticularbetweenthatinterestandthedatasubject'sfundamentalrights, in particular the right to privacy and the right to protection of personal data. Thus, it was held that the right to privacy and the right to personal data overrides the underlying economic and other interests. Court observes, furthermore, that this information potentially concerns a vast number of aspects of his private life and that without the search engine, the information could not have been interconnected or couldhavebeenonlywithgreatdifficulty.Internetusersmaytherebyestablishamore

[145] S and Marper v United Kingdom (2009) 48 EHRR50 para103; Directive95/46 EC(n 4) art 6(l)(e) and Proposed Regulation (n 17) art 5(e)

[146]SupraNote171at 201.

or less detailed profile of the person searched against. Furthermore, the effect of the interference with the person's rights is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such lists of results ubiquitous. In the light of its potential seriousness, such interference cannot, according to the Court, be justified by merely the economic interest which the operator of the engine has in the data processing.

The approach of the ECHR has been to balance the data protection rules and the concerned interests in each case. At times, in absence of the … the court has denied the right of erasure of data. In, Camera di Commercio, Industria, Artigianato e AgricolturadiLeccev.SalvatoreManni[147],thecourtwascalledupontodecideonto decidewhetherthepetitionerMr.SalvatoreManni could stakeaclaim forerasureof personaldata (concerningthebankruptcyofacompanyheadedbyhimfewyearsago) inordertosecuretheirfinancialinterests.Thecourtobservedthatthepotentialclients ofthepetitionershadalegitimateinterestinaccessingtheinformationwhileholding thatthebasicdocuments ofthecompanyconcernedshouldbedisclosedinorderthat thirdpartiesmaybeabletoascertaintheircontentsandotherinformationconcerning the company, especially particulars of the persons who are authorized to bind the company[148]. Hence it was observed by the learned court that the infringement of the interferencewiththepersonaldataofthepetitionerwasjustifiedasthedisclosurewas aimed at serving the legitimate general interest.[149] However, the court did state that theremaybecaseswheretheindividualscouldobjecttheprocessingoftheirpersonal data even when legitimate general interests exist in exceptionally specific situations.[150]

[147]CJEU, C-398/15,CameradiCommercio,Industria,Artigianato eAgricolturadiLeccev. Salvatore Manni, 2017
[148]*Id.*Para60
[149]*Id.*Para56
[150]*Id.*Para61

It can be noted that the court has repeatedly emphasized on the existence of a legitimatepublicinterestbytakingintoconsiderationthetotalityofthecircumstances in each case.

3.2.3 Freedom of the arts and sciences

In*VereinigungbildenderKünstlerv.Austria*[151]wherethedisputeconcernedadispute arising out of a painting that showed nudity and featured a parliamentarian who had prayed for injunction on the grounds of violation of privacy which was duly granted bythedomesticcourt.However,theECtHRobservedthat,thepaintingcouldhardly be understood to address details of [the depicted's] private life, but rather related to hispublicstandingasapoliticianandthatinthiscapacity[thedepicted]hadtodisplay a wider tolerance in respect of criticism.[152]

3.2.4 Freedom of Expression

Article 85 of GDPR governs the relationship between the right to privacy and the freedomofexpression.TheArticlemandatesthestatestoreconcilethetworightsand prescribes several exemption and derogations from different chapters to do so. Prior totheenactmentoftheGDPR,therelationshipbetweenthetworightsweregoverned by the Article 9 of the directive[153]. That being said, it must be noted that the data protectionrightsandthefreedomofspeechandexpressionhavebeenatloggerheads at numerous occasions. The CJEU took the opportunity to define the relationship betweenthetworightsin*Tietosuojavaltuutettuv.SatakunnanMarkkinapörssiOyand Satamedia*[154]whereitheldthatthereisaneedtostrikeabalancebetweenthetwo

[151]V.RICHARDBENJAMINS,POMPEUCASANOVAS,JOOSTBREUKER,ALDO GANGEMI , LAW AND THE SEMANTIC WEB: LEGAL ONTOLOGIES, METHODOLOGIES,LEGALINFORMATIONRETRIEVAL,ANDAPPLICATIONS35-102 (1STWD. 2010).

[152]ExplanationsrelatingtotheCharterofFundamentalRights,OJ2007C303

[153]MikeHintze,*PrivacyStatementsundertheGDPR*,42SEATTLEU.L.REV.1129(2019)

[154]C-73/07,Tietosuojavaltuutettuv.SatakunnanMarkkinapörssiOyandSatamediaOy[GC],16 December2008[Conceptof_journalisticactivities'forthepurposesofArticle9DataProtection

rightsandwhilethefreedomofspeechandexpressionisanindispensibleattributeof every democratic society, in order to strike the balance, the derogations and limitationsoftherighttodataprotectionmustapplyonlyinsofarasstrictlynecessary. Thecourtheld that political debateis an inherent aspect of everyorganicdemocracy and there can't be any justifiable restriction on debates concerning public interest however the editorial gossips that are aimed at satisfying the curiosity of a chunk of readers do not contribute to the debate and there is no underlying public interest. In such cases the freedom of expression can't be expanded to eclipse the right to data protection[155].

In*AxelSpringerAGv.Germany*,[156]aninjunctionorderagainstapublishingcompany that prohibited thereportageofarrest ofa well-knownGerman actorwas challenged the ECtHR on the grounds of the order being violative of Article 10 of the ECHR. The court examined the underlying issue by applying the principle of margin of appreciation and laid a detailed criterion for striking a balance between the right to privacyandfreedomofspeechandexpression[157].Whetherthepublicationcontributes to a debate of general interest; How well known is the person concerned and what is the subject of the report; The prior conduct of the person concerned; The method of obtainingtheinformationanditsveracity;thecontent,formandconsequencesofthe publication; and the severity of the sanction imposed.

In the lights of the facts of the case it was found that sincethe actor was well known to the public and his arrest concerned public interest the injunction posed disproportionaterestrictionsandhenceheldthatthesaidorderviolatedtheArticle10 of the ECHR.

Directive],alsosee,ECtHR,Mosley v.theUnited Kingdom,No.48009/08,10 May2011,paras.129 and 130

[155] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, paras. 81–83.

[156]ECtHR,AxelSpringerAGv.Germany[GC],No.39954/08,7February2012,paras.90and91

[157] CJEU, C-28/08 P, European Commission v. The Bavarian Lager Co. Ltd [GC], 2010CJEU, C-615/13P, ClientEarth, PAN Europe v. EFSA, 2015

3.2.5 Professional Secrecy

Althoughnotafundamentalright,theconceptofprofessionalsecrecyhasdeeprooted underpinningsintheethicalpracticesofeveryprofession.Theprofessionslikeclient-lawyer,doctorpatientrelationsetc.aretrustbasedrelationsandconfidentialityisone ofthevitalaspectsinvolved.TheECtHRhasruledthatitmaybenecessarytoprohibit the disclosure of certain information which is classified as confidential, in order to protectthefundamentalrightofanundertakingtorespectforitsprivatelifeenshrined in Article 8 ECHR and Article 7 of the Charter[158]Thee courts have emphasized on theneedtomaintainbalancebetweentheunderlyinglegitimateinterestsandtherights of the data subjects.

3.3 Important Definitions under GDPR

BeforeanalyzingthevariouscontoursoftheEuropeandata protectionlaw,itwillbe optimum to have a glance at some of the relevant definitions in the GDPR that have had a vital role in shaping the data protection laws across the European Union.

3.3.1 Personal Data

Recognizing the fact that the personal data is of course the most fundamental aspect ofthedataprotection regime. TheGDPR prescribes that any information that can be attributedtotheanypersonorrevealtheidentityofanyindividualisconsideredtobe personal data[159]. The regulation requires the data controllers to take all measures to assess the nature of the information collected[160]. Further, the most important stakeholder of the data is the data subject, the person whose information is being processed.

[158]CJEU,CaseT-462/12R,*PilkingtonGroupLtdv.EuropeanCommission*,Orderofthe President of the General Court, 11 March 2013, para. 44.
[159]*Id.*
[160]CYRUS FARIVAR,HABEAS DATA:PRIVACYVS.THERISEOF SURVEILLANCE TECH 353 (2ND ED. 2018).

3.3.2 Data Subject

Theterm Datasubjectreferstoany identifiablenaturalpersonwhoseindividualdata isbeingprocessed.However,legalpersonscanclaimtheprotectionofArticles7and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons. The right to respect for private life with regard to the processing of personal data, recognized by Articles 7 and8oftheCharter,concernsanyinformationrelatingtoanidentifiedoridentifiable individual.

3.4 Principles of EU Data Protection Regime

Like all well-developed jurisdictions, the European Courts have developed a sound basis of legal reasoning in their pursuit to accord the right of data protection to the greatest possible extent. These principles serve as a parameter for judging the lapses in theright to dataprotection ofthedatasubjects. Notably, theGDPR does retain all these principles to ensure maximum security and control of the data subjects over their data.

3.4.1 Data Accountability Principle

Thethatthecontrollerisresponsiblefor,andmustbeabletodemonstratecompliance with,thepersonaldataprocessingprinciplesthatthecontrollerisresponsiblefor,and should be able to ensure, compliance with the data protection principles. This principle is based on the notion that when the data controllers are held accountable for the breaches.[161]

3.4.2 Data security principle

TheEuropeandataprotectionregimeisbasedtheprincipleofsecuringadequatesecurity andconfidentialityforthedatasubjects.Itencompassestheprincipleofamechanismthat

[161]GeneralDataProtectionRegulation,Art. 24.

ensures that appropriate technical or organizational measures are implemented when processing personal data to protect the data against accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage[162]. The GDPR also requires the data controllers to use, the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons in order to secure the data protection rights of individuals[163]. The GDPR expressly mentions the use of pseudonyms and encryptions for ensuring greater safety. Also, as discussed earlier, the GDPRimposesadutyuponthecontrollerstonotifythedatasubjectswithinagiventime frame about the possible data breaches[164].

3.4.3 The Storage Limitation Principle

The Storage Limitation Principle is also based upon the tenets of securing data security to the greatest possible extent. It mandates that the data ought to be stored only till it is absolutelynecessarytouseit,forweedingoutthepossibilitiesofpotentialbreaches.The GDPRdulyincorporatesthisprincipleandprovidesthatthedatashouldbekeptinaform which permits identification of data subjects for no longer than is necessary for the purposesforwhichthedata[165]iscollected.Also,itprovidesthattimelimitsshouldbe established by the controller for erasure or for a periodic review[166].

In *S. and Marper*[167], the ECHR, observed that retention of the personal data for a disproportionateamountoftimeisnotatraitofademocraticsocietygovernedbythe ruleoflaw.Thecaseconcernedtheretentionofindefiniteretentionofthefingerprints,

[162]Councilof Europe,Committeeof Convention 108,Opinionon theData protection implicationsof the processing of Passenger Name Records, T-PD(2016)18rev, 19 August 2016, p. 9.

[163]GeneralDataProtectionRegulation,Recital39andArt.5(1)(f);ModernizedConvention108,Art. 7

[164] See only art 32 GDPR, ―with its risk-based approach setting out encryption measures as a factor todeterminetheadequatelevelofdatasecurity,orart6(4)(e)GDPR,allowingchangesinthepurpose of processing under certain circumstances.

[165]*Id.*

[166]GeneralDataProtectionRegulation,Recital39

[167] See e.g. *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008

cell samples and DNAprofiles ofthetwo applicants even aftertheiracquittal. These judgments do highlight the European courts with regards to the inherent risks that storageofdatamaypossesstotherighttoprivacyoftheindividuals.Theprincipleis aimed at reducing the data storage by the policy of erasing all the data which have ceased to be absolutely necessary for the purpose for which they were collected. However, the courts have recognized a wide range of exception to the storage principleanddatamayberetainedforpublicinterest,scientificorhistoricalpurposes, or for statistical use, may be stored for longer periods, with a precondition that the data will be used solely for these purposes. In Digital Rights Ireland case[168] while CJEU outlined the need for an objective criterion for issuing data retention directive[169]. The observation was based on the principle that the data ought bot be stored for more than the period for which it is strictly necessary to do so.

3.4.4 Data Minimization Principle

GDPRprovidesthatthedataprocessedmustbeadequate,relevantandnotexcessive inrelationtothepurposeforwhichtheyarecollectedand/orfurtherprocessed.Noting the importance of data minimization, the ECHR in Digital Rights Ireland case, invalidated a provision of data retention directive due to the vast scope of data processing by using a generalized language. The directive provided that the, all individuals and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime[170]. Noting that the directive goes against the principle of barring the excessive processing of data, the court reaffirmed its endorsementoftheprinciplebyobservingthatthe,personaldatawhichisadequate

[168] CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications,MarineandNaturalResourcesandOthersandKärntnerLandesregierungand Others [GC]*, 8 April 2014.
[169]Ibid.Para 63

[170] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications,MarineandNaturalResourcesandOthersandKärntnerLandesregierungandOthers [GC], 8 April 2014

andrelevantbutwouldentailadisproportionateinterferenceinthefundamentalrights and freedoms at stake should be considered as excessive[171].

3.4.5 Purpose Limitation Principle

Ifthe purpose of processing is sufficiently specific and clear, individuals know what to expect and transparency and legal certainty are enhanced. At the same time, clear delineation ofthepurposeis important to enabledatasubjects to effectively exercise their rights, such as the right to object to processing[172]. The principle of purpose limitation has been at the focal point of jurisprudence of European Courts as far as the right to data protection is concerned. Commentators have often hailed this principleasaguarantoroftransparencyandusercontrolasthisprinciplerequiresthat thepersonaldatashallbecollectedforspecified,explicitandlegitimatepurposesand not further processed in a manner that is incompatible with those purposes[173]. The stronglyworded provisionbarsthecollectionandprocessingofdataforfuture,vague uncertainpurposesbyrequiringthatevenforthepurposesthatareancillarytotheone forwhichthedataiscollected,aseparatelegalbasismustexist.Theprinciplethatthe processing of the data may not, therefore, be done in a way that is unexpected, inappropriate or objectionable for the data subject has its genesis in the tenets of purposelimitationprinciple.AspertheOnlyforthepurposesthatarecompatiblewith theinitial purpose,thedatacan befurtherprocessed.Theset ofcompatiblepurposes include, further processing for archiving purposes in the public interest, scientific or historicalresearchpurposesorstatisticalpurposes[174].Thismeansthatevenifthedata obtained by the subject doesn't satisfy the compatibility test, the data controller will be allowed to process the data in these cases. However, the law on the subject as to whatcategoryofdatacanberegardedascompatibleiswellsettledandthefollowing

[171]ExplanatoryReportofModernizedConvention108,para.52;GeneralDataProtection Regulation, Art. 5 (1) (c).

[172]Article29WorkingParty(2013),Opinion3/2013onpurposelimitation,WP203,2April2013.

[173]GDPRArt.4(1).

[174] General Data Protection Regulation, Art.5 (1)(b); Modernized Convention108, Art.5(4) (b). An exampleof suchnationalprovisionsistheAustrian Data Protection Act(Datenschutzgesetz),Federal Law Gazette I No. 165/1999, para. 46

aspects must be considered by the data controller: any link between those purposes andthepurposesoftheintendedfurtherprocessing;thecontextinwhichthepersonal datahavebeencollected,inparticularconcerningthereasonableexpectationsofdata subjectsbasedontheirrelationshipwiththecontrolleronitsfurtheruse;thenatureof the personal data and the consequences of the intended further processing for data subjects;andtheexistenceofappropriatesafeguardsinboththeoriginalandintended furtherprocessingoperation.Theprinciplealsoprescribesthatthedatasubjectshave aright to know the purposes for which their data is being collected and the right to object against collection.

3.4.6 Fairness Principle

The rationale behind the fairness principle is to assure the data subjects that their information shall be processed in a transparent and lawful manner. The principle requires that the data controllers should demonstrate the compliance measures and notifythedatasubjectsaboutthepotentialthreats.Also,whereconsentofdatasubject forms the legal basis of data processing, the controllers are under an obligation to comply with the wishes of data subject[175]. In K.H. and Others v. Slovakia[176], the petitionersweredeniedtheaccesstotheirownmedicalreportsbythehospitalonthe risk of abuse of the data. The ECHR found that the state had failed to show the existenceofsufficientlycompellingreasonstodenytheapplicantseffectiveaccessto information concerning their health. It was held that unless there are compelling reasons to deny the right to access the data to the data subjects, they can't be denied this right.

[175]GeneralDataProtectionRegulation,Art.5(1)(a);

[176] ECHR, K.H. and Others v. Slovakia, No. 32881/04, 28 April 2009; ECtHR, Godelli v. Italy, No. 33783/09, 25 September 2012

3.4.7 Transparency Principle

Nothing assumes more important position in the entire data protection regime of the European union that the element of transparency. The GDPR expressly requires that the data must be processed in a transparent manner in relation to the data subject. The term transparency has been used in the widest sense and it includes, the information given to the individual before the processing starts[177], the information that should be readily accessible to data subjects during the processing[178] and the information given to data subjectsfollowingarequestofaccess totheirowndata[179].*Haralambiev.Romania*[180],is one of the landmark cases where the right to accessibility of the data was highlighted. The petitioner was granted the information held on him after a span of 5 long years, the ECtHRwhilenotingthatArticle8hadbeenviolatedheldthat,individualswhowerethe subject of personal files held by public authorities had a vital interest in being able to access them. The authorities had a duty to provide an effective procedure for obtaining access to such information.[181] It was also held that the defects in the archive section can'tbeaground fordelayingivingtheaccessofdatatothedatasubjects. Also,the Recital 39 to the GDPR expressly provides that the Processing operations must be explained to the data subjects in an easily accessible way which ensures that they understand what will happen to their data. This means that the specific purpose of processing personal data must be known by the data subject at the time of the collection of the personal data. An import theme that runs uniformly across these principles is the effectuation.

3.5 Rights of Data Subjects under GDPR

TheEUlegal orderrecognizes theright ofthedatasubjects to access theirowndata. TheEUCharteroffundamentalrightsexpresslyrecognizestherightofthedata

[177]GeneralDataProtectionRegulation,Article5(1) (a)
[178] CJEU, C-553/07, College van burgemeesterenwethouders van Rotterdam v. M. E. E. Rijkeboer, 2009
[179]CJEU,C-201/14,SmarandaBaraandOthersv.CasaNaţionalăAsigurărideSănătate
[180]ECtHR,Haralambiev.Romania,No.21737/03,27October2009
[181]*Id.*

subjectstoaccesstheirinformationandgetitrectifiedwheneverneeded.TheGDPR lays down a comprehensive right based provisions to give the optimum data control totheindividuals.Infurtheranceofthisobjective,theArticle8mandatesthatawide range of rights that the individuals have as far as their data is concerned. In addition to providing individuals with rights, it is equally important to establish mechanisms that enable data subjects to challenge violations of their rights, hold controllers responsible and claim compensation.

3.5.1 Right to Rectification

Keeping in view the importance of protection of data of the individuals, the GDPR envisages a legal order that seeks to give the data subjects maximum control of their data.Thedatasubjectshallhavetherighttoobtainfromthecontrollerwithoutundue delaytherectificationofinaccuratepersonaldataconcerninghimorher.Takinginto account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement[182]. In *Ciubotaru v. Moldova*[183], where the petitioner was denied the rectification of the name of his ethnicity even in presence of objective evidence in favor of his claim. The court noted that, Preventing the applicant from having his claim examined in the light of objectively verifiable evidence, the State had failed to comply with its positive obligation to secure to the applicant effective respect forhis private life[184]. Thedata controllers are under an obligation to give the data subjects the chance to amend the stored information in a timely manner. In *Cemalettin Canli v. Turkey*, the court regarded the police information report as systematically collected public information stored in files held by the authorities could also fall within the meaning of private life[185].

[182]GeneralDataProtectionRegulation,Article16

[183]Ciubotaruv.Moldova,No.27138/04,2010

[184]ECtHR,CemalettinCanliv.Turkey,No.22427/04,18November2008,paras.33and42–43; ECtHR, Dalea v. France, No. 964/07, 2 February 2010

[185] Similarly, the 14 June 2000 version stipulated that 'Everyone has the right to determine forhimselfwhetherpersonaldataconcerninghimmaybecollectedanddisclosedandhow

3.5.2 Right to Data Portability

Therighttodataportabilityisguaranteedtothedatasubjectsonlyinthecaseswherethe datahasbeenprovidedinpursuanttocontractualobligationsorisbasedonconsent.Cases where the data has been obtained ion legal grounds do lack this right in the EU data protection regime. The data controller is required to develop mechanisms that allow the transmission of data from one controller to the other as per the preferences of the data subjects. The GDPR stresses on the need to develop interoperable formats in order to secure greater data portability.[186]

It may be noted that the regulation doesn't overburden the data controllers with stringent obligations as far as the data portability is concerned. By allowing data to be retained on genuine public interest or in furtherance to the operation of law, the GDPR seeks to balance the interests of data subjects and data controllers. Nonetheless, except for these two compelling circumstances, the right to data portability can't be constricted. It is also apparent that the sole objective behind the recognition of the right is to ensure support user choice, user control and user empowerment, aiming to give data subjects control over their own personal data.[187]

3.5.3 Right to Be Informed

In pursuance of the pursuit to vest the control of data in the data subjects to the maximumextent,theGDPRrecognizes therightofthedatasubjectsto beinformed. The right is based on an assumption that when the data subjects know about the whereaboutsoftheirdata,theoneswhoarecontrollingitandthepurposesforwhich theirdatashallbeused,thedatasubjectsgetbetterplacedinasmuchastheircontrol overdataisconcerned.Thedatacontrollersarerequiredtoinform,theiridentityand habitualresidence,thelegalbasisandpurposeoftheprocessing,thecategoriesof

they may be used'. See CHARTRE 4284/00, 14 and CHARTRE 4360/00, 25 respectively. See further Canmataci and Mifsud-Bonnici (n 13) 10

[186]Recital68totheGDPR

[187]*Id.*

personal data processed, the recipients of their personal data (if any) and how they can exercise their rights under Article 9, which includes the rights to access, rectification and legal remedy[188]. Furthermore, in order to expand the ambit of the volumeofinformationthatthedatasubjectshavewithregardstotheirdata,anyother additionalinformationdeemednecessarytoensurefairandtransparentpersonaldata processing should also be communicated to the data subjects[189].

In order to promote transparency in data processing the GDPR further paces an obligation upon the data controllers to provide information in an easily understandablemannerand to inform thedatasubjects about theways in whichthey canexercisetheirrights.Itrequiresthat,theinformationmustbeconcise,transparent, intelligibleandeasilyaccessible,usingclearandplainlanguage. Itmustbe provided in written form, including electronically where appropriate, and it may even be providedorallyatthedatasubject'srequestandifhisorheridentityisprovenbeyond doubt. The information shall be provided without excessive delay or expense[190].

Further,theGDPRensuresthatthedatasubjectsarewellacquaintedwiththepurpose for which their data is collected and the period for which their data will be retained. It states that the data controller will inform to thedata subjects, the period for which thepersonaldatawillbestored,orifthatisnotpossible,thecriteriausedtodetermine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the datasubjectortoobjecttoprocessingaswellastherighttodataportability,whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data[191]

[188]GeneralDataProtectionRegulation,Recital39

[189] CJEU,C-473/12, *Institutprofessionnel des agents immobiliers (IPI)v. GeoffreyEnglebert andOthers,* November 2013

[190]See,eg.GeneralDataProtectionRegulation,Article5(1)(a)CJEU,C-201/14,

[191]CJEU,C-473/12,*Institutprofessionneldesagentsimmobiliers(IPI)v.Englebert*, 2013

In *Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*[192], where the personal data of the applicants were transferred from one government body to the otherwith thehim being informed,thecourtwhile applying thefairnessprincipleheldthattheinabsenceoflegislativeprocedures (toprotectthe economic interests of the government) such transfer don't get governed by the derogation clause. It was also held that the right to be informed is all the more important since it affects the exercise by the data subjects of their right of access to, and the right to rectify, the data being processed and their right to object to the processing of those data[193].

Under the GDPR, when personal data are collected from the data subject, the controller is obliged to provide the following information to the data subject at the time the personal data are obtained[194]:

- The controller's identity and contact details, including the DPO's details, if any;
- Thepurposeandlegalbasisfortheprocessing,i.e.acontractorlegalobligation;
- Thedatacontroller'slegitimateinterest,ifthisprovidesthebasisfor processing;
- Thepersonaldata'seventualrecipientsorcategoriesof recipients;
- Whether the data will be transferred to a third country or international organization,andwhetherthisisbasedonanadequacydecisionorreliesupon appropriate safeguards;
- Theperiod forwhich the personal datawill bestored, and if establishing that period is not possible, the criteria used to determine the data storage period;

[192]CJEU,C-201/14,*Smaranda BaraandOthersv.CasaNaţionalădeAsigurărideSănătateand Others*, 1 October 2015.
[193]CJEU,C-201/14,*SmarandaBaraandOthersv.CasaNaţionalădeAsigurărideSănătateand Others*, 1 October 2015.
[194]GeneralDataProtectionRegulation,Art.13(1);ModernisedConvention108,Art.7bis(1).

- The data subjects' rights regarding processing, such as the rights of access, rectification, erasure, and to restrict or object to processing; whether the provision of personal data is required by law or a contract, whether the data subject is obliged to provide his or her personal data, as well as the consequences in case of failure to provide the personal data;
- Theexistenceof automateddecision-making,including profiling;
- Theright to lodge acomplaint with asupervisoryauthority;
- Theexistenceoftherightto withdraw consent[195]

The GDPR also casts an obligation upon the data controllers to inform the data subjectsabouttheirrighttocomplaintoasupervisoryauthorityincasesofbreach.[196] OuranalysissofarsuggeststhattheGDPRplacesagreatdealofresponsibilityupon the data controllers in informing the data subjects about every aspect of data processing. However, as noted earlier, there are certain cases where the data controllersareexempted from furnishing theinformation to thedatasubjects[197]. The datacontrollersareundernoobligationtoiftheprovisionofinformationisimpossible or disproportionate, in particular where the personal data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Keeping in tune with the practical aspects of every democratic society, the GDPR accommodatestheviewthatitmaybetooburdensomeandirrationalapproachtoput a blanket ban of non-disclosure of all kinds of information. Issues relating to safeguard national and public security, defense, protection of judicial investigations and proceedings, or the protection of economic and financial interests, as well as private interests which are more compelling than data protection interests and the GDPRgivesthediscretiontothememberstatestorestricttheflowofdata.However,

[195]GeneralDataProtectionRegulation,Art.13and 14

[196]ExplanatoryReportofModernisedConvention108,para. 68.

[197]CJEU,C-201/14,SmarandaBaraandOthersv.CasaNaţionalădeAsigurărideSănătateandOthers, 1 October 2015, paras. 28–46

these restrictions must flow strictly from legislative process and have respect for the fundamental rights recognized by the EU charter, this implies that the domestic law shouldcontainspecificprovisionsclarifyingthepurposeoftheprocessing,categories of personal data included, safeguards and other procedural requirement[198].

3.5.4 Right to Erasure

The right to be erasure or the right to be forgotten is the most recent entrant to the long list of rights recognized by the EU data protection regime[199]. Jurisprudentially, therighttoerasurecanbeviewedasanoffshootofthedataminimizationprincipleas it essentially involves destroying the data that are no longer available. The GDPR recognizes the right to be forgotten in the following circumstances.[200] In *Segerstedt-Wiberg and Others v. Sweden*[201], where the data concerning the political affiliations of the claimants were retained for unreasonable amount of time, the ECtHR found this information could have no relevant national security interest, particularly given its historical nature[202]

In *Brunet v. France*[203] , where the police had retained the information related to the applicant were stored in the criminal data base despite their acquittal, the ECtHR observed that it was intrusiveto the applicant's privacy, as it contained details ofhis identityandpersonality.Inaddition,itfoundthattheretentionperiodforpersonal

[198] *Id.*

[199] SeefurtherDMcGoldrick,*'DevelopmentsintheRighttobeForgotten'*13(4)HRLR761(2013).

[200] The General Data Protection Regulation, Art. 17 (1)provides that: Art. 17 (1)provides that: ―the personal data are no longer necessary regarding the purposes for which they were collected or otherwiseprocessed;thedatasubjectwithdrawstheconsentonwhichtheprocessingisbasedandthere is no other legal ground for the processing; the data subject objects to the processing and there are no overriding legitimate grounds for the processing; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

[201] ECtHR,*SegerstedtWibergandOthersv.Sweden*,No.62332/00,2006

[202] *Id.*

[203] ECtHR,*Brunetv.France*,No.21010/10,18September2014.

records in the database, which amounted to 20 years, was excessively lengthy, particularly since no court had ever convicted the applicant[204].

3.6 International DataTransfer

GDPR, when viewed from the prism of data controllers, appears on the face of it to be strictly tilted in favor of data subjects. While this may be partly true but GDPR does intent to create a legal order that is favorable to free flow of data. The GDPR does take into practical considerations attached to the importance of data in the international trade. In order to ensure that the data subjects are accorded adequate level of protection all over the world, the GDPR lays down several guidelines that ought to be followed in order to transmit data from an EU member state to a non member states[205].

GDPR seeks to regulate the transfer of the of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an internationalorganization.[206]Whilethereisnorestrictionontheflowofdataamongst the member states, the transfer to a third country is subject to the following reservations.

Adequacyofprotection:Article45oftheGDPRprovidesforthemechanismthrough whichdatacanbetransferredtothirdcountries.TheCJEUin*MaximillianSchrems v. Data Protection Commissioner*[207] has held that the adequate level of protection requires the third country to ensure a level of protection of fundamental rights and freedomsthatisessentiallyequivalent.Whileitisnotnecessaryforthethirdcountry tohavethesamepointtopointresemblanceoftheprotectionbutalegalregimethat

[204]*Id.*

[205]See,CommissionCommunicationonExchangingandProtectingPersonalDatainaGlobalized World, COM(2017) 7 final.

[206]GeneralDataProtectionRegulation,Art. 44.

[207] See, CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*[GC], 6 October2015.

isequallycapableasthatofGDPRinitscommitmentfordataprotectionrightsofthe individuals. The European commission has the mandate to assess the domestic laws of the third countries and decide as to if their data protection laws comply with the adequate safeguards' standards.

3.7 The Link between Data Protection Laws and Privacy in the Legal System of European Union

TheArticle7ofEUCharteronfundamentalrightsrecognizesrighttoprivacyasone of the fundamental rights and is supplemented by the right to data protection under Article8.SeveralmemberstatesoftheEUtreattherighttodataprotectionasasubset to the right to privacy and hence don't recognize it as an independent right altogether[208]. However, the mere inclusion of the right to data protection under the chartermustnotbereadasauniformstanceofthememberstateswithregardstodata protection throughout the EU. Unfortunately, there is a negligible reference to the underpinnings of mentioning the data protection rights in the charter[209]. In order to assesstheneedbehindcreatingaseparaterightintheformofrighttodataprotection, the section shall strive to establish a link between the right to privacy and data protection laws. Following are the ways in which the relationship between the two rights can be established.

- RighttoPrivacyandDataprotectionareseparateandyetcomplimentary rights.
- Dataprotectionrightisasubsetoftherighttoprivacyforallpractical purposes.
- Thedataprotectionrightisanindependentrightwithabroaderambitthan the right to privacy.

[208] Federico Ferretti, The Foundations of EU Data Protection Law, 2 EUR. DATA PROT. L. REV. 278,(2016).

[209] JA Cannataci and JP Mifsud-Bonnici, Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty (2005)

Thesectionshallalsotakeintotheaccounttheinterpretationbythe European Courts of Human Rights regarding the overlapping meanings of the both rights. It may be noted that the data protection rights offer the individuals a greater control over their personal data as compared to the right to privacy for all practical purposes.[210]

3.7.1 Right to Privacy and Data Protection are Separate Yet Complimentary Rights

The proposition that the data protection laws are a set of instruments aimed at protectingthehumandignityoutlinesoneofthemostnormativefoundationsfortheir recognition as a fundamental right. The 1983 Population Census Decision is one of theearliestjudicialprecedentsthatrecognized therights ofindividualstocontrolthe flow of their data[211]. While holding that the right of individual self-determination of their information finds its genesis in the right to human dignity.[212] In the case of *NetherlandsvParliament*,theCourtheldthatthefundamentalrightstohumandignity must be observed while disallowing the patentability of the human organs. Another credibleargumentinthefavorofthemodelcanbetracedintheinclusionoftheright tohumandignityintheEUcharterwhichrecognizesitasoneoftheinviolableaspects of life. The data protection laws and the right to privacy appear to be collectively fostering the right to human dignity and individual liberty,

However, there still exists certain ambiguity about the dignity-based conception of thedataprotectionlawsduetheirnon-inclusioninthebasedrightschapteroftheEU charter[213].Itmaybesafelyconcludedthatthedraftersofthechartersdidnotrecognize data protection rights as a human dignity based right.

[210]M.-P.,andIrion,K.(2018)._Therighttoprotectionofpersonaldata:thenewposterchildof European Union citizenship?‘ in: de Vries, S., de Waele, H., and Granger, M.-P., eds., Civil Rights and EU Citizenship

[211]PopulationCensusDecision,1BvR209/83,BVerfG65,1.

[212] Kevin McGillivray, Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU, 17 TUL. J. TECH. & INTELL. PROP. 217, 254 (2014).

[213]NationalPanasonicvCommission[1980]ECRI-2033,paras18–20

3.7.2 Data Protection Laws as a Subset of Right to Privacy

One of the most accepted views regarding the nature of relationship between data protection laws and the right to privacy revolves around the conception that the data protectionlawsareasubsetoftherighttoprivacy[214].Thisviewhasgarnered alotof academicandlegalbasisinthepastfewyearsandtheproponentsofthistheoryhave regarded the data protection laws as one of the latest developments to the evolution oftherighttoprivacy[215].It isarguedthatthedataprotectionlawsdonotcatertoany other rights that are not related to the concerns of the protection of privacy of the individuals in one way or the other. The reasoning that the right to privacy had been recognized as a right to be left alone and with the advancement of technology such right can't be preserved without the data protection laws seems plausible. As per Solves, the data protection laws and the right to privacy are the members of a family which resemble each other but are not identical[216].

3.7.3 Right to Privacy and Data Protection Rights are IndependentRights

The report of the Expert Group on Fundamental Rights, Affirming Fundamental RightsintheEUcanberegardedasoneofthemostnotableendorsementsoftheview that the data protection laws are an independent right altogether. The report recognized the right to determine the sue of personal data as a complementary right totherightssetoutunderArticle2to13oftheUNHCR[217].Thismodelsuggeststhat although both, the right to privacy and data protection rights seek to ensure informational privacy, their scope varies considerably. Gutwirth argues that the purposesservedbythedatapersonal lawsarefargreaterinnumber andamplitudeas

[214]RightsinConflict-ReconcilingPrivacywiththePublic'sRighttoKnow,63LAWLIBR.J. 551, 563 (1970).

[215]NetherlandsvParliamentandCouncil[2001]ECRI-7079.

[216]RouvroyandPoullet,_TheRighttoInformationalSelf-determination(n11)47

[217] See, Technical Report on the Review of the European Data Protection Directive: accessed 5 August 2019, the RAND report the Directive therefore serves a number of purposes, privacy protection being only one

compared to the privacy laws and vice versa[218]. It is argued that the data protection lawservesamultitudeofpurposesandoneofthemistheprotectionofprivacyofthe information of the users. The provisions of the data protection laws that are not concerned with the right to privacy deal with other aspects of data security that are far broader in their amplitude.[219]

This model can be regarded as the closest one to the constitutional framework of severalmemberstatesthatconsiderrighttoprivacytobeanindependentrighttagged with the right to privacy. For example, the French data protection law is anchored around the notion of individual liberty whereas the data protection laws of Germany treat human dignity as an indispensable aspect of human life[220]. The analysis of the propositions of all the three models suggest that there still is a dearth of an all-encompassingexplanationastohowthedataprotectionlawsandrighttoprivacyare related to each other.

3.8 Reading the Right to Data Protection under the Article 8 of the ECHR

The right to privacy is recognized under the Article 8 of ECHR.[221] The European Court of Human Rights have interpreted the right to be privacy in a much a much flexible manner as compared to the approach of characterizing it as a right to be let alone. However, the right to privacy is not recognized as an unqualified right under the convention and Article 8(2)permits interference in the right as per the procedure establishedbylaw.[222]Hence,inordertodeterminetheapplicationofArticle8ofthe ECHR, few important questions need to be answered. First of all, the courts try to determineifat allthereexistsanyinterestprotectedunderArticle8(1)oftheECHR. Ifsuchanyinterestexists,hastherebeenanyunwarrantedinterferencewiththose

[218]DeHertandGutwirth,_DataProtectionintheCaseLawofStrasbourgandLuxemburg(n8)8.
[219]SusanNevelowMart,TheRighttoReceiveInformation,95LAWLIBR.J.175,190(2003).
[220] Judy Meadows; Bob Oakley, Balancing Act - Reconciling Privacy with the Public's Right to Know, 8 AALL SPECTRUM 14, 35 (2004).
[221]SeeSamuelWarrenandLouisBrandeis,TheRighttoPrivacy(1890)IVHarvardLawReview193
[222]Article8(2)ECHR,allowsinterferencewithitsexercisewhentheinterferenceisin accordance with the law and is necessary in a democratic society

interests?[223]Thissectionofdiscussionshallbeconcernedwiththeextent ofinterests guaranteedbythedataprotectionlawswhichareprotectedbyArticle8oftheECHR.

InordertoattracttheapplicationoftheArticle8(1)ofECHRthepetitionersmustbe abletoshowthattheirinterestsconcerningprivateandfamilylife,thecorrespondence and the home is affected. However, the ECtHR has taken a broader view of the term private life by while including video surveillance images[224], email sent from the work[225],trafficdataonphonecalls[226]initspurview.Precedentssuggestthatthecourts have not given any weightage to the decisive nature of the information. In its landmarkjudgmentin*SandMarpervUK*[227],theCourtobservedthatwhileassessing whether a personal information falls within the private-life aspect of the Article 8 of ECHR,dueemphasishastobegiventothespecificcontextinwhichsuchinformation have been recorded and retained. The judgment also outlines the stance taken by the courts to rely on the non-exhaustive parameters in order to determine the nature of data.Thecourthasalsoheldthatthedatathatisinpublicdomaincanalsobetreated as a private data as the zone of interaction between an individual and public at large is well within the scope of private life.[228]

The factual circumstances of every case are taken into consideration while determiningtheextentofallegedinterferenceoftheinterestsrecognizedunderArticle 8(1) of ECHR. At times, the Court has treated the mere storage of data and its subsequencedisclosuretotheemployeesofthepetitionersasaviolationofrightto

[223] Beate Roessler, _Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy in Beate Roessler and Dorota Mokrosinska (eds), Social Dimensions of Privacy: Interdisciplinary Perspective (Cambridge: Cambridge University Press 2015)

[224]PerryvUnitedKingdom(2004)39EHRR3.

[225]CoplandvUnitedKingdom(2007)45EHRR 37.

[226]Malone(n83)para64

[227]SandMarpervUK(2009)48EHRR 50.

[228]GoodwinvUnitedKingdom(2002)35EHRR18,para 90

privacy. The court held that the mere storage of data of an individual amounts to the breach of right to privacy irrespective of the motive behind such storage.[229]

3.9 The New Data Protection Law Regime

The Need for GDPR

The issue with the Directive is that it's no longer relevant to today's digital age. Itsprovisions fail to address how data is stored, collected, and transferred today—adigital age. Like many regulations and statutes throughout the EU and U.S., theseregulations haven't been able to keep up with the pace of the levels of technologicaladvancement.

Data is becoming very valuable for today's economy and are essential to daily lives ofthecitizens.Thenewrulesofferauniqueopportunityforbusinessesandthepublic alike. Businesses, especially the smaller ones, will be able to benefit from the innovation-friendly single set of rules and put their houses in order in terms of personal data to restore consumer's trust and use it as their competitive advantage acrosstheEU.Citizenswillbeabletobenefitfromthestrongerprotectionofpersonal data and gain better control over how the data are handled by the companies.[230]

Directive 95/46/EC was replaced by the new data protection regime known as the Generaldataprotectionregulationfrom25th May2018[231]TheEuropeanunion adoptedtheGDPRon16th May2016andthusreplacedovertwodecadesolddata

[229] International Review of Law, Computers & Technology 73; and Maria Tzanou, Data Protection as a Fundamental Right Next to Privacy? ―Reconstructing a Not So New Right (2013) 3 International Data Privacy Law 88

[230] ITGP Privacy Team (2017). BU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition. IT Governance Ltd.

[231]TheRegulationhasbeeninforcesince24May2016andwasapplicablefrom24thMay2018.

protection directive[232] along with the police directive[233]. The new rules promise a better data protection mechanism for protection of data of every individual and company operating within the EU irrespective of their place of origin. This part of deals with the underlying principles behind the new regulations and the impact that they will have on the stakeholders.

The underlying reason behind the well-established legal framework regarding data protection in the EU is based on the two important factors:

1. The need to modernize the data protection laws in order to keep them in tandem with the needs of the modern world.
2. Strengthening the individuals' control over their data by recognizing the data protection right as a fundamental right.

The GDPR has been hailed as a bold step towards strengthening the right to data protection by endorsing it as a fundamental right for the EU.

These rules are set to ensure greater uniformity and thus allow the businesses throughout the EU to explore new opportunities by reinstating the trust among their customers.Theguidelinesarisingoutofasinglesetofruleswillalsomakewayfora mucheasierflowofdataamongstthememberstates[234].Attheonset,itmustbe clarifiedthattheGDPRdoesn'tmakeanynotabledeparturefromthedataprotection directive and follows its objectives in pith and substance. However, these guidelines do incorporate the principles laid down in various judicial precedents on the subject andhenceofferasetofguidelineswhicharesuitedforthemodernday.Theinclusion

[232] Directive 95/46/EC of the European Parliament regarding the processing of personal data of theindividualsandtheirfreemovementanditwasadoptedon23rdNovember2015,OJL281of 23.11.95.

[233] Directive (EU) 2016/680 the regulation dealt with the powers of the authorities to process the information for investigation, detection and prevention of crimes and had repealed the council framework decision 2008/977/JHA, OJ L 119, 4.5.2016.

[234]KevinMcGillivray,*ConflictsintheCloud:ContractsandCompliancewithDataProtection Law in the EU*, 17 Tul. J. Tech. &Intell. Prop. 217 (2014).

of several benign elements in the guidelines vouch for greater control of the individuals over their data.[235]

3.10 Better Protection of the Data and New Opportunities for the Businesses

In the erstwhile data protection regime, the member states have applied the Data protection directive differently and as a result in lot of cases inconsistencies used to arise amongst the laws of two different states. Perhaps, the greatest incentive of GDPRwillbeuniformityandconsistencyamongstthelawsofmemberstatesthrough this one shop stop mechanism.

The GDPR also promises a level playing field for the companies doing business in theEuropeanmarkets.Itlaysthatthesameruleswillbeappliedtothecompanieswho transactintheEUirrespectiveoftheirplaceoforiginandhencepaveswayforamuch moreuniform and even regime. Thedetailedguidelines on theareaseem to leaveno roomforambiguityasregardstotheapplicationoftheprovisionsonanycorporation that is even a virtual stakeholder in the European markets.

As per the Directive 95/46/EC, these guidelines are aimed at addressing the issues related to the data protection from the scratch[236]. Moreover, they set out a range of innovative remedies against any breach thereof.

OneofthemostnotablechangesthattheGDPRwillbringtotheforeistheimmensely greater control of the individuals over their personal data. The regulations had expandedtherightoftheindividualsovertheirpersonaldatabyrecognizingtheright toportability.Thiswouldmeanthattheindividualswillbeallowedtoletthe

[235]Mike Hintze, Privacy Statements under the GDPR, 42 Seattle U. L. Rev. 1129 (2019)
[236]Article29 Working Party(2005),Working documenton acommon interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November 2005.

companies transfer their personal data under a contract[237]. This will ensure free flow of data and hence it will be much easier for the common man to which between different companies for better handling and security of their data. Moreover, this is boundtoincreasethecompetitionamongstthecompaniesandthustheinterestsofthe individuals will be served better.

The guidelines also lay down a comprehensive road map for remedies against the breach of data. Notably, it clearly defines what will constitute Data Breach[238]. Also, it imposes a duty upon the companies to inform the individuals whose data is likely to be breached in a specified time frame[239]. Once, it becomes apparent that the potential data breach may have an impact upon the fundamental rights of the individuals, the concerned company is required to communicate the same to the supervising authority within 72 hours from the incident. The guidelines also provide for a detailed and organized mechanism to prevent any potential breach of data and requires that adequate technological measures are taken in order to prevent any infringementofrightsoftheindividuals.[240]Also,thesupervisoryauthorityisrequired to takeactions in atimely mannerin orderto mitigatetheimpending risks[241]. Thisis certainly going to ensure effective redressal and greater protection of data of the individuals.

[237] *Id.*

[238] Art.30GDPR

[239] "It should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation"

[240] Article 29 Working Party (2004), Opinion 10/2004 on More Harmonized Information Provisions, WP 100, Brussels, 25 November 2004.

[241] LilianEdwards,*Privacy,SecurityandDataProtectioninSmartCities:A Critical EU Law Perspective*, 2 Eur. Data Prot. L. Rev. 28 (2016)

These guidelines ensure that there exists effective governance to implement these rules in letter and spirit by providing for a comprehensive remedial procedure.[242]

3.11 Rights and Obligations of Individuals under GDPR

Whileaswehavenotedinourdiscussionssofarthattheregulaysdownextensive guidelinesforprotectionagainstthedatabreach,italsoimposesobligationsuponthe individualsanddatacontrollersaccordingly.Barringfewexceptions,thethemeofthe regulation revolves around securing the maximum protection of the rights of individuals.Weshallnowlookindetailthekindsofrightsthattheseguidelinesseek to confer upon the data subjects.

3.11.1 Right to be forgotten

UnderArticle17 ofthe GDPR, theRight to beforgotten, also termedas the Right to erasureisgrantedtotheindividualsincertaincases.Thismeansthattheyhavearight to get their data erased/deleted from the controllers after making a request for the same in the following scenarios. The purpose for which the data was collected has been accomplished. The consent for processing of data has been withdrawn by the individual. There isn't any underlying legitimate interest in retaining the data that exceeds the interest in its deletion.

3.11.2 Right to portability of Data

Righttoportabilityofdataisoneofthemostnotablerightsreorganizedbythe GDPR which will have the practical benefits for the commoners in as much as their control overdatais concerned[243].Thiswillmeanthat theindividualswillbeabletotransmit theirpersonaldatafromonecontrollertotheotherinanytransmittablemedium.This

[242]AsangWankhede,*DataProtectionin India andtheEU: Insights inRecentTrends and Issues in the Protection of Personal Data*, 2 Eur. Data Prot. L. Rev. 70 (2016).
[243]Lina Jasmontaite, *European Union: The European Data Protection Supervisor (EDPS) Opinion 4/2015 Towards a New Digital Ethics*, 2 Eur. Data Prot. L. Rev. 93 (2016).

will enable the users to use their data for availing multiple kinds of services even by submitting their data to any controller.[244]

3.11.3 Right to Information

The recital to Article 12, the principle of transparency requires that any information addressedtothepublicortothedatasubjectbeconcise,easilyaccessibleandeasyto understand, and that clear and plain language and, additionally, where appropriate, visualization be used. Such information could be provided in electronic form, for example,whenaddressedtothepublic,throughawebsite.TheGDPRguaranteesthe right to the data subjects the right to know the purpose for which their data is being collected and processed[245], the right to know the period for which their data will be retained[246]andperiodforwhichsuchretentionwillbeinexistence[247].Theregulation requiresthedatacontrollerstorenderallthisrequiredinformationtothedatasubjects in an understandable and plain language.[248]

3.11.4 Right to Seek Remedy

The GDPR envisages a Data Protection Regime that keeps the importance of informational self-determination at the helm. This is amply reflected in the provisions providing for the remedies in cases of breach of the personal data of the individuals. It provides in the clearest of the terms the right of the data subject to initiateallthe proceedingsintheappropriatecourtswillbeindependentofone'sright to lodge a complain with the Data Protection Authority[249]. It further provides that authorityshallkeepthedatasubjectinformedabouttheprogressofthecomplaint

[244]Recital68toArticle20,—Wheretechnicallyfeasible,thedatasubjectshouldhavetherighttohave the personal data transmitted directly from one controller to another

[245]*ECtHR,K.H.andOthersv.Slovakia,* No.32881/04,28April2009;ECtHR,Godelliv.Italy, No. 33783/09, 25 September 2012

[246]SeeFurther,LauraF.Edwards,*RightsThatMadetheWorldRight*,102Judicature15(2018)

[247]GeneralDataProtectionRegulation,Art.4(11).SeealsoModernizedConvention108,Art.5 (2).

[248]GeneralDataProtectionRegulation,Art. 7.

[249]GeneralDataProtectionRegulation,Art. 77.

and the alternative legal remedies[250]. Further the regulation provides that the data subject shall havethenecessary recourse against the dataprotection authority in the eventofeverybindingdecisionoftheauthorityagainstthem.Furthertheschemeof theprovisionsoftheGDPRrecognizetherightofthedataprincipalstoseekremedy against the breaches without any impediments.

3.12 Data Protection in the UnitedStates

The United States, unlike the European Union doesn't have a standardized and uniform data protection legal regime in place. The country has enacted several enactments in order to secure the data protection rights of the individuals to the maximum possible extent[251]. These laws are extremely specific in their scope and subject matters and cover very limited industry participants. While, it is outside the scopeofthisresearchtocoverallthedataprotectionlegislationsintheUnitedStates at the federal and the state level, the following section will strive to outline the underlyingthemeoftheselegislations.AfterexploringthemandateofAfewnotable data protection enactments will be taken up to explore the quality of protection that have been conferred to the individual in the United States.

Apart from these specific enactments that seek to regulate the processing of data the conceptofrighttobeleftalonecanbegatheredfromtheconstitutionaswell.Oneof the earliest cases where the Supreme Court took a broad view of the fourth amendment and held that it protected people and not just the places from the state's intrusionswas*Katzv.UnitedStates*[252].However,thecourtdidn'trecognizetheright toprivacyisaseparateright.Itwasonlyafterthecase *Whalenv.Roe*that herightto privacy was recognized as the right to privacy as recognized as a separate constitutionalright,theSCheldthatethrighttoprivacyinfactinvolve[s]atleasttwo differentkindsofinterests.Oneistheindividualinterestinavoidingdisclosureof

[250]GeneralDataProtectionRegulation,Art.78.

[251]SGUTWIRTH,DATAPROTECTIONINAPROFILEDWORLD,210(1ST ED.2010).

[252]Seee.g.,Olmsteadv.UnitedStates,277U.S.438,464(1928)

personalmatters, and anotheristheinterestinindependenceinmakingcertainkinds of important decisions[253].

3.12.1 The Right to Privacy in UnitedStates

No study about the evolution of right to privacy as a distinct right in the US can be justified without mentioning the ground breaking Article The Right to Privacy by… The propositions of the work have proved to be a beacon of eternal light to anyone who is interested in the development of the right to privacy as a separate right in the UnitedStates[254].However,theassertionsabouttherightofindividualstobeletalone had previously been made by the judiciary but the authors of the article were successful in drawing a close association between the right to life and the right to privacybystrikingthecollectiveconscienceofthepolicymakersandthecivilsociety at large. Before we delve further in the process of evolution of right to privacy as a distinct right, it will be optimal to discuss the series of judicial pronouncements that havecreated thejurisprudential basisforrecognitionof Rightto Privacyin America.

What lies at the core of justification of recognition of right to privacy as a distinct rightistherecognitionofintangibleharmstothehumanmind.[255]Thoughts,emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature. In one of the earliest cases on intrusion into the privacy of an individuals' life, the New York court had issued an injunctionagainstthepublicationofaphotographofanactresswhileperformingina theatre while terming it an unwanted intrusion in the person life[256].

[253]SamuelD.Warren;LouisD.Brandeis,*RighttoPrivacy*,4Harv.L.Rev.193(1890-1891).

[254] Daniel J. Solove, A Brief History of Information Privacy Law, in PROSKAUER ON PRIVACY § 1-4 (2006) (citing DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 1 (1972)).

[255]HerbertSpencerHadley, *RighttoPrivacy*,3N.W.L.Rev.1(1895).

[256] GWENKENNEDY,DATAPRIVACYLAWANDPRACTICALGUIDE432-433,(2ND, LSP PRADHU ED., 2018).

One of the most vociferous challenges that the recognition of right to privacy faced was the assertion that the torts like libel and defamation more or less cover the same set of injuries that the right to privacy claimed to address and provide a remedy against. However, it is important to note that the torts of libel, slander, defamation etc. do provide remedy against the damage to the reputation of an individual in the eyesofthesocietyandincasethepetitionerisunabletoprovesuchinjury,theclaim doesn't subsist. Butwhat right to privacy seeks tocater is the personal pain inflicted on one's feeling. That branch of the law simply extends the protection surrounding physical property to certain of the conditions necessary or helpful to worldly prosperity. On the other hand, our law recognizes no principle upon which compensation can be granted for mere injury to the feelings.

AsperJusticeYates,*itiscertaineverymanhasarighttokeephisownsentiments,if he pleases. He has certainly a right to judge whether he will make them public, or committhemonlytothesightofhisfriends"*[257].Whateverbethemodeofpublication, thecommonlawhasalwaysbeenconferringrightupontheindividualstocontrolwhat they wish to publish to the rest of the world and what they wish to keep with themselves.Takeforexample,Amanwritealettertohisgirlfriendabouthisfeelings for her, even if a third person obtains the possession of the letter, he doesn't get the right to publish the contents of the letter to the world. What does the law seek to protect here?

The principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of theintellectoroftheemotions,istherighttoprivacy,andthelawhasnonewprinciple toformulatewhenitextendsthisprotectiontothepersonalappearance,sayings,acts, and to personal relation, domestic or otherwise.

[257]*Id.*

3.12.2 The Children's Online Privacy Protection Act (COPPA)[258]

Children are by far one of the most populous consumers of the internet today. A lot ofgaming,chattingandeducationwebsiteshavechildrenasthegreatershareoftheir consumer segment.[259] The ever-evolving presence of the children as the online consumers creates room for the breach of the privacy of the children (a lot of whom aren't capable of understanding the implications of the submitted information). For long, a lot of jurists across the country have pitched for strict federal regulations for protecting the privacy rights of the children and the Children's Online Privacy ProtectionActisthemanifestationofthesepropositions.TheCOPPAwasenactedin 1998 to ensure protection of the collection, storage and processing of the personally identifiable information of the children. This section shall deal with the underlying concerns that triggered the enactment of the Act and then move on to examine the extent of parental consent under the Act and thus examine the feasibility of the resolutionstoprotecttheprivacyinterestsofthechildren.TheimpetusoftheActcan be traced to an investigation report. by the Federal Trade Commission in the alleged breaches in handling the information by KidsCom.com which highlighted the need for a comprehensive regulation to highlight the risks associated with the online submission of the information and the need for parental consent in any such disclosure.[260]

Mandates of COPPA:

The COPAA is aimed at informing the children and their parents about the information collection, storage and processing policies of the websites that they are using. It requires that the consent about the submission of information must be obtainedfrom theparents andthey mustbegiven achancetoreviewtheinformation

[258] 15U.S.C.6501–6505

[259] Melanie L. Hersh, Is COPPA a Cop Out? The Child Online Privacy Protection Act As Proof That Parents,NotGovernment,ShouldBeProtectingChildren'sInterestsontheInternet,28FordhamUrb.L.J. 1831 (2001). Available at: https://ir.lawnet.fordham.edu/ulj/vol28/iss6/4

[260] DawnA.Edick,RegulationofPornographyontheInternetintheUnitedStatesandtheUnitedKingdom: A Comparative Analysis, 21 B.C. INT'L & COMP. L. REV. 437 (1998).

and limit such information.[261] The regulations provide for a reasonable standard of complianceincollection,storageandprocessingofdata.TheActregulationsareaimed atprotectingthechildrenbyregulatingthewebsiteoperatorsandonlineserviceproviders. The term operator has been very broadly defined in the Act and it encompasses any onlineserviceprovideroperatingforcommercialpurposes.Anotherimportantaspect oftheActisitsdefinitionofthetermdirectedatchildrenanditmustbeconcededthat the definition is broad enough to encompass all the websites which the children potentially use. All the websites that have a dedicated are for children, the subject matterofthewebsiterelatesto childrenarecategorized asdirectedtowardschildren.

The Act also provides for a broader definition of the term Personally identifiable information[262]andprovidesforinclusionofalltheinformationthathavethepotential of disclosing the personal details of any individuals. Any information such as the email address, the name, thecontact details, social security number, resident address andotherancillaryinformation.Moreimportantly,theuseofthepersistentidentifiers (suchasthecookies)havealsobeenidentifiedasPII.[263]Anothernotableaspectofthe Actistheobligationonthepartoftheoperatorstomaintaintheconfidentialityofthe furnished information. It is required that the operators must have a detailed mechanismtoprotecttheinformationprovidedbytheuserswhichmustincludefixing responsibility for the breach of confidentiality, ensuring adequate security of data through use of encryptions, firewalls and passwords. It can be gathered from the wordings of the provision that the act requires the websites to take reasonable steps to prevent any breaches.

3.12.2.1 Scope of parental consent

Themostcriticalaspect oftheActisno doubtthe processof obtainingthe verifiable parentalconsentastherelevanceofthelegislationliesontheitspracticality.Asper

[261]Id.

[262]Thomas B. Nachbar, Paradox and Structure: Relying on GovernmentRegulation to Preserve theInternet's Unregulated Character, 85 MINN. L. REV 215 (2000)

[263] Jay Krasovec, Cyberspace: The Final Frontier, For Regulation?, 31 AKRON L. REV. 101, 115(1997)

the Act, the operator must obtain verifiable parental consent before collecting any information from the children. The Act aims at giving the parents the full authority overthecollectedinformationandtheoperatoris boundtoinformtheparentsbefore makinganymaterialalterationtothecollecteddataandrevealingthesaidinformation with a third party.

However, the Act does provide several relaxations and exceptions to the rule of obtainingparentalconsent.Keepinginviewthehardshipsthatcouldresultoutofthe strict compliance to the above rule, the websites are at the liberty to get the payment done through the parents, make a toll-free parent call, send a verification mail to the parents among other things. Also, the Act also exempts the websites from obtaining the parental consent for collection of information on a one-time basis.[264] However, forfurthercommunication,thewebsiteisunderanobligationtotakereasonablesteps to obtain the verifiable consent of the parents. In the cases where it is necessary for thewebsitetoobtainthenameandotherdetailsofthechildrenforsecuringthesafety of the child, the obligation may be done away with.

Another important aspect of the parental consent is the mode of its obtaining. Opinionsonthelegislativeintentonthemodeofcollectingtheconsentoftheparents vary and a lot of jurists are of the opinion that the email verification may not be adequately safe mode of obtaining the parental consent and it ought to be supplemented by other steps as well.[265] However, there is a very little scope for switching back to the print and send method of approval, as this may substantially increase the transaction costs and adversely impact the businesses. Unfortunately, in spite of all the benign intentions behind the regulations, the Act doesn't take into consideration the practical commercial realities. As one of the commentator's notes

> *"COPPA'sparentalconsentmeasuresaredifficulttoimplementandcostlyto realize.Print-and-sendmethodsareantitheticaltothespeedandefficiencyofe-*

[264]SeeC.F.R.§312.5(c)(2)

[265]JoshuaWarmund,CanCOPPAWork-AnAnalysisoftheParentalConsentMeasuresinthe Children's Online Privacy Protection Act, 11 Fordham Intell. Prop. Media & Ent. L.J. 189 (2000).

commerce. Ill Postal, fax, and credit card fees, when aggregated, can be substantial." Although some companies are developing new technologies to comply with the Act, the end-product usually makes browsing a painfully slow and laborious process. Indeed, companies will need to hire and compensate personnel to oversee and implement these new policies. As a result, the offline labor associated with these methods is prohibitive, for both parents and operators[266]".

It is no doubt true that the COPAA intends to protect the interests of the children and their personal information online by making strict regulations for the website operators but these guidelines do seem far from the practical realities as there is a high likelihood of children manipulating the consent of their parents. In absence of a full proof way of obtaining the parental consent, the changes sought to be brought by COPAA may be minimal.

3.12.2 Electronic Communications Privacy Act(ECPA)

The Electronic Communications Privacy Act had for long been projected as the pole star in the dark skies of the privacy regime of the US. Several commentators have time and again retreated that the ECPA was one of the first laws in the US to have provided for a detailed framework for protection of the privacy of the users online[267]. With the advent of emails and other digital modes of communication meant that the exchanges in the course of communication could be recorder and further accessed by the third parties. Moreover, the judiciary was of the view that the information voluntary submitted for business purposes didn't get the protection of the fourth amendment. In the wake of growing usage of email and the internet, a good chunk of policy makers were propelled to come up with a piece of legislation that protected the privacy of users in these communications. The genesis of the ECPA can be traced in the Office of Technology's assessment report that highlighted the grave risk to the individual liberty in the digital communications. However, the technological world has undergone a sea of changes from 1986 till today and there looms a challenge over the relevance of the Act in providing

[266] Id.

[267] Anne Eisenberg, What's Next; Memories as Heirlooms Logged into a Database, N.Y. TIMES, Mar. 20, 2003, at G6

adequate protection to the users from the existing threats online. In this section, we shall first have a look at the genesis of the Act and then examine whether the ECPA has been successful in keeping up with the pace of time. Among many suggestions that the report made was the extension of the protection guaranteed to the conventional first-class mail to all the digital communications.

3.12.3 Fair Credit Reporting Act(FCRA)

The Fair Credit Reporting Act is a comprehensive code aimed at regulating the consumercreditratingagenciesandtheretailcreditbureau.Thesereportingagencies have the access to the credit history of the millions of Americans through their Associatedcreditbusinessbureau.Everytransactioninvolvesseveralpartiessuchas the lender, the borrower and a credit rating agency that decides upon the credit worthinessoftheborrower.Itisofcommonpracticeforthebanksandotherfinancial institutions to rely upon the credit score of the loan applicants for sanctioning the loans and notable is the fact that the credit score is obtained by a cumulative assessment of a wide range of information about the background of the applicant[268]. Keepinginviewthebulkoftheinformationthatliesinthesefiles,thethreattoprivacy becomes an ever-growing risk attached to the industry. The following sections will discuss the measures that the FCRA seeks to bring in to protect the financial privacy of the consumers.

The most notable change the FCRA brought was the remedies against the false information furnishedby thecredit agencies. Priorto theenactment, aconsumerhad no remedy against any inappropriate report provide by the credit rating agencies nor did arise any cause of action against any unauthorized disclosure of such information[269].TheActrequirestheratingagenciestoestablishanotificationsystem to inform the consumers about the existence of information about them. This obligation the part of the lenders to notify the consumers about the information that isusedagainstthemgivesthemanopportunitytoknowandifpossible,challengethe

[268] *Id.*

[269] See,e.g.,Watwoodv.Stone'sMercantileAgency,194F.2d160(D.C.Cir.1952)

information. The Act also imposes a duty upon the rating agencies to inform the consumers about the details of the information. One of the other ways in which the FCRA seeks to guarantee the privacy of the consumers is by assuring the confidentiality of the data. Before the enactment of the Act, there were several instances in which the entities which did not have a genuine business interest in the information were also able to get this information with impunity. The doctrine of conditional privilege was used largely to mask the breach of right to privacy.

3.12.4 Health Insurance Portability and Accountability Act(HIPAA)

Theessenceoftherighttoprivacyisreflectedinthestate'sabilitytoensureyouthat thedatawhichyoudon'twishtorevealtoothersremainsunderyourcontrol,it'syour right to be left alone. While it has been an ethical medical practice to ensure the privacy of the fiduciary relationship between the doctors and patients, the era of digitalization has emerged as one of the greatest risks to the medical privacy. The Health Insurance Portability and Accountability Act aims at safeguarding the protected health information of the citizens all over the United states from potential breaches. The Act bars all the health care providers from disclosing any information aboutthecitizenswithouttheconsentoftheindividuals.[270]Followingaresomeofthe notable aspects of the Act concerned with the protection of privacy

- Sharing of Protected health information to the individuals: Once requested, theinstitutionsmustsharetheinformationwiththeapplicantsinalimitedtime frame[271].
- ThePHImay bedisclosed forthe purposes of treatment andpayment[272].
- Theinstitutionmustnotifyanypotentialbreachofdatatotheconcerned individuals[273].

[270]Id.§§164.104,164.306,164.502

[271]See,e.g.,*Univ.ofColo.Hosp.v.DenverPub.Co.,340*F.Supp.2d1142,1143(D.Colo.2004) (holding that no private right of action exists under HIPAA).

[272]*Id*

[273]SamuelD.Warren;LouisD.Brandeis,*RighttoPrivacy*,4Harv.L.Rev.193(1890-1891).

The code nonetheless doesn't recognize right to privacy s a fundamental right protected by the constitution; all it guarantees is a greater level of protection against unlawful disclosure of the medical history of the patients while recognizing an existence of legitimate privacy interest of the individuals in such data. The fact that the medical history includes sensitive information about the medical and health backgroundoftheindividualsmakestheirprotectionanindispensableaspectofright to privacy. An excerpt from the federal register amply reflects the recognition accorder to the right to privacy.

> *"Privacyisafundamentalright.Assuch,itmustbevieweddifferentlythan any ordinary economic good. The costs and benefits of a regulation must, ofcourse,beconsideredasameansofidentifyingandweighingoptions.At the same time, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom. A right to privacy in personal information has historically found expression in American law. All fifty states today recognize in tort law a common law or statutory right to privacy. Many states specifically provide a remedy for public revelation of private facts. Some states, such as California and Tennessee, have a right to privacy as a matter of state constitutional law. The multiple historical sources for legal rights to privacy are traced in many places, including Chapter 13 of Alan Westin's Privacy and Freedom and in Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995). Throughoutournation'shistory,wehaveplacedtherightsoftheindividual at the forefront of our democracy. In the Declaration of Independence, we asserted the "unalienable right" to "life, liberty and the pursuit of happiness." Many of the most basic protections in the Constitution of the UnitedStatesareimbuedwithanattempttoprotectindividualprivacywhile balancing it against the larger social purposes of the nation".*[274]

[274]JoanM.Kiel,*TheHealthInsurancePortabilityandAccountabilityAct(HIPAA) Implementation Via Case Law*, 20 J. Contemp. Health L. &Pol'y 435 (2004).

Interestingly,theActdoesnotseektoregulateallthe medicalrelationshipsandonly those interactions that fall under the definition of covered entities are regulated[275]. Several commentators do consider the patients, the covered entities and the business organizationsasthethreestakeholdersrepresentinganequilateraltriangletoformthe beneficiaries of the Act. In the following sections, the definition of all the three entities will be discussed in a nutshell followed by an examination of the other relevant aspects.

Patient: As per the Act, the any person who submits the Individually identifiable health information is said to be patient. The information may range from the name, address, medical history etc. of the subject. As one of the commentators have put it "Individuallyidentifiablehealthinformationisafancy,verbosewayofdescribingall information that in any manner may identify the individual who has received health careservicesorcouldbeusedtoidentifythatindividual.[276]Interestingly,theHIPAA applies to all kinds of written as well as oral communications to ensure that no loopholes exist.

Business Associates: The entities associated with the covered entities (such as the lawyers, accountants, assistants etc.) fall within the category of business associates. As per the code, Business associates" are those businesses, individuals, and entities that are required, as a part of the function and/or service performed for a covered entity, to have access to and knowledge of individually identifiable health information[277].

Covered entities: The most important stakeholders in the sojourn for ensuring the privacy of the health records of the patients are the covered entities. The HIPAA regulates the Health care service providers, the health plans and the health maintenance organizations. The onus of complying with the mandate of the Act lies on these covered entities and they are required to appoint a compliance officer to ensure non-disclosure of the sensitive information related to the patients.[278]

---

[275] *Burgerv.LutheranGeneralHospital,* 759N.E.2d533(Ill.2001).

[276] *Arbsterv.UnemploymentComp.Bd.ofReview*,690A.2d.805(Pa.1997)

[277] *Id.*

[278] *Id.*

Curbing the growing instances of the private dissemination of the confidential medical information in the absence of legitimate business interest remains to be the mostvitalaspectoftheHIPAA[279].However,inthewakeofpracticalrealities,theAct doesn't prohibit legitimate health information sharing in the ordinary course of businessinordertopromotethediscussionsamongthehealthcareproviderstocome up with the most optimal treatment plans for their patients.

3.12.5 Video Privacy Protection Act,1998

TheVideoPrivacyProtectionAct,1988hasbeen inalimelightforquiteawhiledue to a surge in the lawsuits under the law against Netflix and Twitter in recent years. TheVPPAseekstopreservepersonalprivacywith respecttotherental,purchase,or delivery of video tapes or similar audio visual materials[280] The Act bars the audio-visualdigitalserviceprovidersfromdisclosingpersonallyidentifiableinformationas includ[ing] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider. information related to their consumers to a third party without their expressed approval. Despite numerous technological changes in past three decades, the relevance of VPPA in protecting the rights of the consumers due to liberal interpretation of the Act. In re Hulu Privacy Litigation, a US district court held that the online video streaming serviceprovidersalsocomewithinthemeaningofvideotapeserviceproviders[281].In *Stanely v Georgia*[282], the court recognized the right to even receive obscene material in one's private premises.

TheprovisionsoftheActhaveforlongbeenassociatedwiththefirstamendmentand timeandagainithasbeenarguedthatabsenceofsuchfreedomswouldseverely

[279]StandardsforPrivacyofIndividuallyIdentifiableHealthInformation,65Fed.Reg.82,462,
[280]MarcChaseMcAllister,ModernizingtheVideoPrivacyProtectionAct,25Geo.Mason L.Rev.102(2017).
[281]VideoPrivacyProtectionActof1988,Pub.L.No.100-619,102Stat.3195(1988)(codified at18U.S.C.§2710).
[282] Marc Chase McAllister, *Modernizing the Video Privacy Protection Act*, 25 Geo. Mason L.Rev. 102 (2017)

inhibit the intellectual and liberal thought process.[283] It is notable that the provisions of the Act which could have potentially become redundant in the onslaught of revolutionary technological changes have held their ground firmly in the wake of liberal interpretation by the judiciary[284]. Following are some of the drafting lapses which have been a bone of contention

LocusStandi:ThequestionastowhomaysueunderVPAAhasbeenatthehelmof affairsregardingthedraftinglapsesintheAct.ThewordingsoftheActremainvague ondecidingtheliabilityofthereceiverofthedisclosedata.Amajorityofthecourts have held that only the service provider can be held liable under the Act on the grounds that these platforms which store the information in bulk can leak detailed records of an individual's reading materials, purchases, diseases, and website activity.[285]

Personally Identifiable Information (PII): In what is termed as the most flexible explanationofthetermPersonallyIdentifiableInformation,thefirstcircuitcourtheld that, PII constitutes of information reasonably and foreseeably likely to reveal, directly or indirectly, an individual consumer's identity[286]. The interpretation provides for a reasonable foreseeability test and thus goes on to lay that any informationwhichislikelytodisclosetheidentity ofthepersonmay beclassifiedas aPII.InreHuluPrivacylitigation,thedistrictcourtobservedthatevenabarcodethat has the potential of disclosing the personal information of an individual can be held to be a PII. However, just because an information can be processed and tapped into an identifiable information doesn't make it a PII[287].

[283]See*Yershovv.GannettSatelliteInfo.Network,Inc*.,820F.3d482,484

[284]See*Dirkesv.BoroughofRunnemede,* 936F.Supp.235,238(D.N.J.1996)

[285]*Mollettv.Netflix,*Inc.,795F.3d1062,1065(9thCir.2015)(statingthatthenewspaperdetailed 146 films that the Bork family had rented from an area video store)

[286]InreHuluPrivacyLifig.,2012WL3282960,at*6.

[287] See In re Nickelodeon, 827 F.3d at 284, 290 ("In our view, personally identifiable information under the [VPPA] means the kind of information that would readily permit an ordinary person to identify a specific individual's vido-watching behavior.").

However,theVPAAdoesprovidecertainexceptionstotheruleofnon-disclosureand allows the service providers to disclose the information that is incidental to the ordinary course of business.[288] Also, the Act doesn‘t provide for any penalty against thebreachesandonlyprivatecauseofactionscanariseoutofanyviolationunderthe Act. In *Austin-Spearman v. AMC Network Entertainment LLC, the court held that,* wrongful disclosure even without additional injury [afforded] a right to relief[289].

In *Camfield v. City of Oklahoma City*[290], an Oklahoma citizen complained that the academy award-winning German movie *The Tin Drum* contained child pornography and therefore violated Oklahoma law. The police took the film to a local judge, who informally viewed it and agreed that it was probably child porn. The police subsequently went to neighborhood video stores and removed all copies of *The Tin Drum*,andobtained,withoutawarrant,thenamesofthosewhowerecurrentlyrenting it. One copy had been rented by a local ACLU employee who got wind of the impending seizure and wanted to see if the movie was really objectionable. Police cameto Mr.Camfield's houseand asked forthecassette,which hehanded overafter some discussion of "the artistic merits of the movie. The court found that the city violated Camfield's rights under the VPPA by obtaining his rental records without a courtorderorwarrant.HewasawardedthestatutoryminimumofS2500andavictory for civil liberties.

3.12.6 Family Educational Rights and Privacy Act(FERPA),1974

The family educational rights and Privacy act of 1974 is one of the most specific federal privacy laws of the United States as it aims to protect the purely educational recordsofthestudentsacrossthecountry.Thetermeducationalrecordhasavery

[288] *Albrightv.Rodriguez*,51F.3d1531,1534(10thCir.1995)

[289] See Austin-Spearman v. AMC Network Entm't, LLC, 98 F. Supp. 3d 662, 669-70 (S.D.N.Y. 2015) (adopting this view of the VPPA and requiring VPPA plaintiffs to engage in an "ongoing relationship with the provider initiated by the plaintiff's own actions")

[290] Cf *Camfield v. City of Oklahoma* City, 248 F.3d 1214, 1220-21 (10th Cir. 2001). The district court had allowed suit against the recipients of personally identifiable information. While this determination was not appealed, the Tenth Circuit Court of Appeals did not sua sponte revers

wideconnotationanditincludesallthematerials,documentsandinformationthatare directlyrelatedtoanystudentstudyingintheUSandareunderthepossessionofany educational institution. As far as the scope of the Act Further the term educational institution includes any public or private agency or institution which is the recipient of funds under any applicable program. The Act aims at vesting the control all the academic information of the students with them and their legal representatives and thus bars any unauthorized disclosure of any such information with third party. It mainlyconfersthreedistinctrighttothestudentswithregardstotheirdatawiththeir educational institution.

Righttoauthenticateandamendtheinformationatanytime: Theactlaysdown detailed procedures for the redressal of any grievances related to the student's data.

Righttocontroltherecipientsofthedata: TheActbarstheeducationalinstitutions fromhaving apolicythat deniestheaccessoftheseinformationtostudents andtheir parents.

Right to challenge and review any information: The authorities are under an obligationtoactonthereviewrequestswithin45 daysfailingwhichacomplaintcan be lodged with the education department.

These rights against disclosure of data to the third party and bar on any policy that aims at denying the disclosure of the information[291] to the students and their parents areaimedatsecuringthestudentsdatatothegreatestextent.However,theconsentof thestudentsandtheirrepresentativesdoeshavesomeexceptionsandtheeducational institutionsmaynotrequireany consentbeforedisclosureunderthesewindows.The schools may disclose the data to officials with legitimate educational interest, or the bodies that are conducting researches for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instructions.Also,ifthe datafallswithinthedirectoryinformation,andastudenthas

[291]20U.S.C.§ 1232g(b)(1)(A).

not opted out of it under a reasonable amount of time, the information can be disclosed.

The Act also provides that the institutions are bound to give the students an opportunity to the students to challenge the authenticity of their data on the grounds of the records being inaccurate, misleading, or otherwise in violation of the privacy rights of students. The Act also provides appropriate remedies for any breach of provisions of the Act by providing for appropriate action against the concerned institution.However,theviolationsoftheserightshavenotbeencriminalizedbutthe appropriateactionsarelimitedtowithholdingoffundsandterminatingeligibilityfor future funds.

The scheme of provisions do suggest a half-hearted commitment by the state to protect the personal data of the students in as much as the breach of the provisions aren'tcriminalizedhoweveritdoesseemthatthesectionsoftheActdoprovideample protectionagainstanymisuseofdataofthestudentsbytheeducationalinstitution.It is worthwhile noting that the Act doesn't guard against the possible breach of the obligations to store this information safely.

3.12.7 GrammLeachBlileyAct,1999

The Financial Services Modernization Act of 1999 Act, also popularly knownas the Gramm Leach Bliley Act seeks to provide a prudential framework for the affiliation of banking institutions.[292] One of the key aspects of the Act is its emphasis upon the FinancialPrivacyofthecustomerswhichwasmost unaddressedhithertothepassing oftheAct.[293]TheActprovidesforaTheFinancePrivacyRuleswhichformapartof the Act lay are modeled upon the principles of informed consent and informational self-determination.Theserules,interalia,governthemannerandextentofcollection, storageandprocessingofthefinancialdataoftheconsumersbythefinancial

[292] What is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Bliley Act in 2019, Digital Guardian (2021), https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

[293]CorinneCrawford;BoroughofManhattanCommunityCollege,TheRepealOfTheGlass-SteagallAct AndTheCurrentFinancialCrisis"(PDF).JournalofBusiness&EconomicsResearch,2011,pp.127–133

institutions. Notably, these rules also apply to the entities which receive these data irrespective of the fact whether they are financial institutions or not.

Acommonthemethat bindstherulesistheemphasisupontheprincipleofinformed consentthroughtheprovisionfornoticeateachstepofprocessingofpersonaldata.[294] The rules mandate that the financial institutions are bound to notify the clients explaining what information is being collected, why is it being collected, where will itbestoredetc.[295]Additionally,thefinancialinstitutionsaredutyboundtoinformthe customers about the changes, if any in the privacy policy of the institution while givingtheclientsanoptiontooptoutatanytime.TheActalsoprovidesforpenalties as well as punishment in cases of breaches.

3.12.8 Non-Solicited Pornography and Marketing Act,2003

TheControlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM)Actof2003isafederalActthataimstoregulatetheinter-statecommerceby imposing limitations or punishments on unsolicited communications by e-email or Internet.Thelegislationwasenactedasaresponsetotheunprecedentedgrowthinthe instances of spam mails as a marketing tool. The Act specifically defines a "commercialelectronicmailmessage"tobe"*anyelectronicmailmessagetheprimary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose*).[296]"

The Act lays down detailed limitations upon the unsolicited commercial email by banning false of misleading header information. It also inter alia prohibits the usage of deceptive subject lines and mandates that every unsolicited commercial has to be tagged as “advertisement” while availing the option to the recipients to opt out of receivingthee-mailsinfuture.[297]TheActalsoenjoinstheresponsibilityuponthe

[294] Ibid.

[295]PhilGramm,"DeregulationandtheFinancialPanic, 2017-08-11attheWaybackMachine,opinion pages of *The Wall Street Journal*, published and retrieved on February 20, 2009

[296]ControllingtheAssaultofNon-SolicitedPornographyandMarketingAct,NationalCreditUnion Administration (2021), https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/controlling-assault-non-solicited-pornography-and-marketing-act

[297]Ftc.gov(2021),https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf

FTCtoissuerules regulatingandlabellingtheSexuallyexplicitemails as such.The legislation may thus be considered to be an extension of the right to not receive unsolicited communications as an aspect of informational self-determination.

3.12.9 Federal Trade Commission Act,1914

TheFederalTradeCommissionAct,1914establishedtheFederalTradeCommission, thebodywhichhastheauthoritytoenforceallthefederalPrivacylegislationsthatwe have previously discussed including the Non-Solicited Pornography and Marketing (CAN-SPAM)Act,Gramm-Leach-BlileyAct,theEqualCreditOpportunityAct,the FairCredit Reporting Act to nameafew.[298] TheCommission derives itspowerfrom theSection5oftheActwhichempowersitto preventunfairmethodsofcompetition and unfair or deceptive acts or practices in or affecting commerce.

TheActalsoallowstheCommissiontopenalizetheentitiesthatthatviolatetheirown policies by false advertising and other actions that can harm consumers. The agency uses a wide set of tools to achieve its objective of securing consumer privacy. These toolsincludepolicyinitiatives,consumerandbusinesseducationtocreateawareness about the evolving aspects of data privacy. The commission uses its long standing experience and expertise in the data protection arena to assist the . federal and state legislatures and U.S. and international government agencies to improvise the data protection regime in the country.

3.13 Data Protection in the United Kingdom

TheUnitedKingdomisconsideredtohaveamoreliberaldataprotectionframework than most of its erstwhile EU counterparts. The earliest data protection enactment in thecountrycanbetracedbackto1984.However,itwasonlytheDataProtectionAct of1998thatacomprehensivecodefortheprotectionoftherights ofthecitizenswas enacted, it recognizes eight principles that must be followed by the data controllers for data processing. These principles are famously known as the Data Protection Principles. They are

[298] Ibid.

1) The personal data ought to be processed lawfully. Unless the conditions prescribedintheschedule2arecompiled,nodatacanbeprocessed,alsointhecases of sensitive data, at least one of the conditions of schedule 3 must be met.

2) Onlyforthelawfulpurposes,thepersonaldataofthedatasubjectsshould be processed. Also, the data must not be processed for the purposes other than for what it is obtained.

3) Thepersonaldatacollectedmustnotbeexcessiveforthepurposeitisbeing collected.

4) Thedatacontrollerisunderanobligationtokeepthedatauptodateand accurate.

5) Thedatashall notbe processedin violationtotherightsof thedata subjects.

6) Thepersonaldatashallnotbestored fortheperiodlongerthan theperiod for which it is absolutely necessary for the purposes for which it was collected.

7) Thedatatransfertoathirdcountryisnotpermittedunlessthatcountry affords adequate amount of data security.

8) Appropriatemechanismsmustbeputinplaceto preventtheinstancesof data breaches

It is quite apparent that our discussions about the features of GDPR have also highlightedthesamesetofprinciples.Itmaybenotedthatthedataprotection actsin United Kingdom have been in tune with the European data protection regime ever since the emergence of the concept of data protection.

3.13.1 Features of the Data Protection Act of 2018

The purpose behind enactment of the 2018 Act is twofold. First to implement the provisions of the GDPR in the domestic arena and to modernize the data protection laws to bring them in resonance with the challenges to the data protection rights in thecurrentscenario.FollowingaresomeofthequintessentialfeaturesoftheUKData protection laws.

3.13.1.1 Resolve for Protection of Personal Data

The applied GDPR (provisions of GDPR) with certain modifications and the 2018 Act form the basis of the data protection laws in the UK as of now. The Act applies to the processing of all kinds of personal data.[299] As the provision expressly reads, it must be read as a supplementary of the GDPR and envisages a regime that accords almostsamelevelofprotectiontothedatasubjectsasthatofGDPR.Notably,theAct retains all the definitions of the GDPR in letter and spirit and does not propose any alterations.[300]Otherterminologiessuchas theDataSubjects,thepublicauthorityetc. havebeen incorporated from the GDPR with minimal alterations from the GDPR.[301]

Notably,theActprovidesacompletelydifferentframeworkforsafeguardsbylawto theautomateddecisionmaking.Itconcernswithsignificantdecisionsbasedsolelyon automatedprocessingthatareauthorisedbylawandsubjecttosafeguardsforthedata subject's rights, freedoms and legitimate interests.[302]

TheActdefinestheterm significantdecisionas:

a) Adecisiontheycanmanifestintolegaleffects
b) Adecisionthat affectstherightsof thedata subjectsin asimilar manner.

TheActprescribesthatwhenadatacontrollertakesasignificantdecisionthatisbased onlyontheautomatedprocessingmechanism,theyareunderanobligationtonotify

[299]Part2,Chapter1oftheDataProtectionAct,2018coversthetypes
(1) ThisPartisrelevanttomostprocessingofpersonaldata.
(2) Chapter2ofthis Part—
(a) applies to the types of processing of personal data to which the GDPR applies by virtue of Article 2 of the GDPR,
(b) supplements,andmustbereadwith,theGDPR.
(3) Chapter3ofthis Part—
(a) appliestocertaintypesofprocessingofpersonaldatatowhichtheGDPRdoesnotapply (see section 21), and
(b) makesprovisionforaregimebroadlyequivalenttotheGDPRtoapplytosuchprocessing

[300]Part2,Chapter1

[301]Seeeg.Adriana-MariaSandru;Daniel-MihailSandru,*HumanitarianLawand Personal Data Protection*, 2018 Pandectele Romane 58 (2018).

[302]DataProtectionAct2018,Sec.14

inwriting,thedatasubjectsaboutsuchdecisioninareasonableamountoftime.This provision is aimed at giving the data subject a chance to request for a revision of the decisions.However,theActreducestheprotectiongrantedunderArticle15(1),15(2) and 15(3) of the GDPR (concerning the confirmation of processing, access to data and safeguards for third country transfer)[303]. As per the Act, these protections shall extendonly to the financial transactions in absenceof acontraryintention expressed by the data subject earlier.[304]

3.13.1.2 Transfers of personal data to third countries

The Act vests in the secretary of the state, the power to specify, circumstances in which a transfer of personal data to a third country or international organisation is to betakentobenecessary forimportantreasonsofpublicinterest.Itmaybenotedthat the same provision vests in the secretary the power to determine the question as to whether the third country offers adequacy of protection for the purposes of Article 45(3) of the Act.[305] Almost all other aspect of the Act are on the lines of the GDPR withoccasionalalterationstomaketheprovisionsmorecompatiblewiththedomestic needs.[306] In the next section, we shall consider the possible implications of the BREXIT on the data protection laws in UK.

3.13.2 Brexit and GDPR

TheUKDataProtectionAct,2018seekstomodernizetheprovisionsofthe1998Act by incorporating the changing aspects of the data protection arena. The Act is also aimed at implementing the GDPR with certain modifications in the legal order of UnitedKingdom.GiventhefactthattheUKhaslefttheEU,theGDPRshallceaseto applytoitanditwillbetreatedasathirdcountryforthepurposesoftheregulation.

[303] *Id.*

[304] DataProtectionAct2018,Sec.12(1) b

[305] DataProtectionAct2018,Sec.18(2)a

[306] Ico.org.uk.2020.*DataProtectionAndBrexit*.[online]Availableat:<https://ico.org.uk/for-organisations/data-protection-and-brexit/>

As already discussed in the previous section[307], in order to pave ways for exporting data into the UK from the member states of the EU, the country must demonstrate that adequate level of protection exists.

The United Kingdom and the European Union have to chalk out the Brexit Deal by October 2020, a deadline which is most likely to get extended. However, until the dealisstruck,theGDPRwillcontinuetoapplyintheUnitedKingdomaswell[308].The finderwouldliketopointoutthattherearenomaterialdifferenceswhatsoeverin the approaches of the GDPR and United Kingdom in their approach towards data protection[309] and hence it is not deemed proper to reengage in the same analysis.

Theanalysisofsomeofthenotablelegislationsrelatingtothedataprotectionlawsin the United States do come across as a potential tool to secure the rights of the individuals to have complete control over their personal data. However, some of the important lacunas that have emerged are as follows

Unlike the European Union that has a comprehensive code in the form of General Data Protection Regulation, the US has too many data protection laws with every limited scope. As a result, the data protection framework in the country is quite complex,technicalandvast.Also,thereareseveralstatelawsandfederallawsonthe same subject matter which leads to unnecessary confusions.

- Most of the enactments (at least a majority of them) were enacted over two to three decades ago and as a result of enormous technological developments a lotoftheseguidelinesdostruggletoaddressthechallengesposedinthe

[307] GDPR Associates. 2020. *GDPR And Brexit - Does The UK Still Need ToComply?*. [online] Available at: <https://www.gdpr.associates/gdpr-brexit/>

[308]Bird&Bird.2020.*Brexit:DataProtectionAndCybersecurityLawImplications*.[online]Available at: <https://www.twobirds.com/en/news/articles/2016/uk/brexit-data-protection-and-cyber-security- law-implications>

[309]*Id.*

modern era. Hence there is a pressing need to incorporate the aspects of technological developments in order to serve the purpose of securing data privacy for the citizens.

- Despite these shortcomings, it must be admitted that the United States does havein placean effectiveand robust framework to securethedataprotection rights of the individuals. However, the data protection regime in EU is way ahead, advanced, comprehensive and modern as compared to that of US.
- TheEuropean Union has somenatural edgein the field of data protection due to the following two reasons. First being the absence of a comprehensive federal law to regulate processing of data in US in contrast to the EU which has perhaps the most individual centric data protection law in the world. The secondreasonistheapproachofliberalinterpretationoftheEuropeanCourts towards the issues concerning data protection.
- Also, thereis aneed to haveacomprehensivefederal lawin theUnitedStates on thelinesoft the General DataProtection Regulation to effectively cater to the challenges of the modern day.
- India has been time and again described as the most important of shoring businesslocationintheworld[310]anditwasduetotheever-expandingnetwork of the data offshoring companies in India that marked the herald of the concerns of potential data breaches in India. It is often said that but for the threatsofbreachofinformationalprivacyasanoutcomeofthedataoffshoring companies, India would never have had required a data protection regime at all[311].Withnolegalframeworkinplacetoregulatethedataoffshoringprocess in India, there were numerous instances of data theft and breaches of informational privacy by these offshoring companies[312].Of course, these incidentsdidn'tgounnoticedbytheinternationalmediawhicheventuallyput pressure on the Government of India to enact data protection law.

---

[310] *Id.*

[311] Silvia Lucia Cristea &Viorel Banulescu, *The Right to Personal Data Protection. The Right to Privacy.AComparativeLawApproach*,64 AnaleleStiintifice Ale Universitatii Alexandru Ioan Cuza Din Iasi Stiinte Juridice 1 (2018).

[312] *Id.*

Sincethefinderhasidentifiedthekeycomponentsofarobust Data Protection Regime in the countries with advanced Data Protection law framework, an optimum platform for a thorough analysis of the existing law in India on the subject has been made. The finder has so far identified the best practices adopted by different jurisdictions in imparting a fair degree of protection to the personal data of the citizens and the challenges faced by the governments in effectively tackling the privacy issues that are related to technological developments.Theoutcomeofthechapterhasenabledtheauthortoalsoidentify a threshold of protection that a digitalized society expects as far as the issue of informational privacy is concerned.Hence the forthcoming chapter seeks to obtainacomprehensivepictureoftheexistingDataProtectionlegislationinIndia.

CHAPTER4:DATA PROTECTION REGIME IN INDIAN LEGAL SYSTEM

4.1 Introduction

ThePreviouschapterhasequippedthefinderwithaverybroadunderstandingof the different approaches adopted by the European Union, the United States and the United Kingdom towards protection of Personal Data. Before getting into the discussionsabouttheoptimalityofacertainDataProtectionModelinIndia,itwould benecessaryto have athorough reviewoftheexisting dataprotection legislations in India. The sole objective of the discussions in this chapter is to strike gather the best possible understanding of the state of Data Protection in India.

Theworldisbecomingmoreandmoreintensely digitalizedbyeachpassingdayand Indiais no exception to thephenomena[313]. With billions ofpeopleall overthe world communicating with each other through the transmission of information through digitalmediumsahugevolumeofdataisgeneratedallovertheworld.Thenewfound digital mediums of communications including the social media intermediaries such as theWhatsApp, Facebook, Twitterand otherplatforms have an extensiveoutreach amongst a huge chunk of population[314]. With the availability of cheaper internet and broader connectivity, the more than 53% of the Indian population has an online presence[315].

Further, the use of online payment applications such as the Paytm and Google pay havegotanextensivepresenceintheIndianeconomy[316].Theuseoftheseappsby

[313]TheHindu.2020.*WhatIsTheRightWayOfRegulatingSocialMedia?*.[online]Availableat: <https://www.thehindu.com/opinion/op-ed/what-is-the-right-way-of-regulating-social-media/article29291424.ece>

[314]*Id.*

[315]Mandavia,M.,2020. *IndiaHasSecondHighestNumberOfInternetUsersAfterChina:Report*. [online] The Economic Times. Available at: <https://economictimes.indiatimes.com/tech/internet/india-has-second-highest-number-of-internet-users-after-china-report/articleshow/71311705.cms?from=mdr>[Accessed28May2020].

[316]*Id.*

thecitizens have added to theenormous amount ofdatathat is involved in thedigitals sphere. However, the progress in technology has also armed both the public and privatesectorentitiesto getaccess tothepersonal dataoftheindividuals,storethem and process them within a matter of moments[317].

A surge in the internet users also indicates that a lot of personal and financial data is usually involved in thesetransactions. The immense popularity of these applications amongst the Indian users, make India a hotbed of digital transmissions[318]. It must be noted that these mobile applications that offer various kinds of services to the uses suchasonlinechatting,digitaltransactions,onlineshopping,cabserviceetc.dostore and process a huge volume of the personal data of the individuals[319].The evolution of a digital economy with the Data at its Centre-stage can be amply traced in the following excerpt:

Something as simple as hailing a taxi now involves the use of a mobile application whichcollectsandusesvarioustypesofdata,suchastheuser'sfinancialinformation, her real-time location, and information concerning her previous trips. Data is fundamentallytransformingthewayindividualsdobusiness,howtheycommunicate, and how they make their decisions. Businesses are now building vast databases of consumer preferences and behaviour. Information can be compressed, sorted, manipulated,discoveredandinterpretedasneverbefore,andcanthusbemoreeasily transformed into useful knowledge[320].

Alongwiththecollectionandprocessingofthepersonaldata,theprocessmoreoften thannotinvolvesstorageandtransmissionofthepersonaldata.Withtheadvancement oftechnology,thestorageandprocessingofpersonaldatahasbecomeextremely

[317] *Id.*

[318] The Hindu. 2020.*India'S Digital Transformation*. [online] Available at: <https://www.thehindu.com/opinion/op-ed/indias-digital-transformation/article8224206.ece>

[319] *Id.*

[320] *Id.*

viableoptioneconomicallyandtechnicallyaswell.Thesephenomenaensurethatthe data aggregators not only collect bit also store the personal data of the individuals which can be used to make the individual profiles of the users, of course for a more efficient functioning of the applications. The creation of customized user profiles helpstheserviceproviderstoreducethetransactiontimeandmaketheservicesmore efficient. The online aggregators and the e-commerce companies make use of the online history ofthe users to suggest the products that the users may be interested in buying[321]. To be precise, the use of data can have a great impact on the way things work in the digitalized world and every entity, whetherbe it the private sector or the public sector, does strive to get the maximum output through the data of their users. Use of data for analyzing the locations of people living in a particular area may be used to improved trafficconditions[322], theanalysis ofhealth dataofthepatients may helpthefindercomeupwith abetterdiagnosisprocedure[323],theanalysisofthe demography and economic condition of the individuals can be of great help to the governmentinframingpoliciesandtargeteddeliveryofsociallybeneficialpolicies[324]. Theprocessingofdatacanalsobeofgreathelptothefinancialregulatorsindetecting frauds and the law enforcement agencies prevent crimes[325]. There has been an increasing trend among the law enforcement authorities to use drone cameras and using more complex methods of surveillance with the help of the internet and sophisticated technologies[326].

[321] *TheSolutionsState:WhyTheDigitalNeedsTheHuman*.THEINDIANEXPRESS(Feb.2020) <https://indianexpress.com/article/explained/the-solutions-state-why-the-digital-needs-the-human-5625290/>

[322] *SomeReformsInIndiaShowBenefitsOfDigitalisation:IMF*,THEECONOMICTIMES,(July, 2020) <https://economictimes.indiatimes.com/news/economy/policy/some-reforms-in-india-show-benefits-of-digitalisation-imf/articleshow/68806028.cms?from=mdr>

[323] *Id.*

[324] *Id.*

[325] *State Of Privacy India*, PRIVACY INTERNATIONAL (Aug. 2019) <https://privacyinternational.org/state-privacy/1002/state-privacy-india>

[326] *DataProtection:WhyAComprehensiveLawIsNeeded*(June2020)THEFINANCIALEXPRESS, <https://www.financialexpress.com/opinion/data-protection-why-a-comprehensive-law-is-needed/1694205/>

However, while making things convenient for the users, and providing for a safer society, the storage of the personal data of the individuals possesses a great threat to the informational privacy at the same time[327]. An increasingly prevalent use of the internet has thrown open a plethora concerns related to the possibility of data breaches.With government being the largest processor of personal data in India, it becomes extremely important to have a law in place that would regulate the entire affair of collection, storage and processing of the data and put in place necessary safeguards. However, the threat to the informational privacy in India, just like the entire world is not something that has just loomed up, it is just that the threat has become much more larger with the advent of digitalization[328].

With the development of science, Information and Communication Technologies through the computer and other electronic instruments have greatly enhanced our capacities to collect, store, process and communicate information. At the same time, it makes us vulnerable to intrusions of our privacy on a larger scale. This privacy invasionmayhappenfromthepersonalspherealso.Itmayhappenthroughanyofthe following ways:

- dataonourownpersonalcomputerscancompromiseusinunpleasantwayswith consequences ranging from personal embarrassment to financial loss[329],
- transmissionofdataovertheInternetandmobilenetworksisequallyfraughtwith the risk of interception[330],
- inthisageofcloudcomputingwhenmuchofourdata,e.g.ouremails,chat logs, personalprofiles,bankstatementsetc.,resideondistantserversofthe companies whoseservicesweuse,ourprivacybecomesdependentontheinternalelectronic security systems of these companies[331]

[327] *Id*
[328] *Id.*
[329] SubhajitBasu,*Policy-Making,TechnologyandPrivacyinIndia*,6IndianJ.L.&Tech.65(2010).
[330] *Id.*
[331] *Id.*

- theprivacy of children, women, old persons,and minorities tendto beespecially fragile in this digital age as they have become frequent targets of exploitation[332], and
- online data handling has procreated new kinds of annoyances such as electronic voyeurism, spam or offensive email, 'phishing' etc., and each of these can affect the privacy of any individual[333]

4.2 The Information Technology Act,2000

TheIndianInformationTechnologyAct2000("Act")wasabasedontheModelLaw onElectronicCommerceadoptedbytheUnitedNationsCommissiononInternational TradeLawthesuggestionwasthatallStatesintendingtoenactalawfortheimpugned purpose, give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. As noted earlier, the scheme of data protection laws in India was initially hinged at the affairs related to the off-shoring businesses and the information technology sector[334]. It was the result of the void in the existing laws in India that there were severalinstancesofdata theftandamidstgrowinginternational pressure, Indiacame up with the Information Technology Act, 2000 to regulate the flow of data in the country. Even to this date, the IT Act remains the most foundation of the several Indianlawsaimedatsecuringasocietyconducivetothecauseofdataprotection.The boost in the technological sector marked the beginning of a data driven culture in India and it was through the problems outlined above are regulated primarily by the IT Act. The Act has been amended several times till now in order to tackle the ever-evolvingchallengesposedtothesecurityofdatawiththeadvancementoftechnology.

[332]RaghunathAnanthapur,India'sNewDataProtectionLegislation,8SCRIPTed192(2011)

[333] Lothar Determann & Chetan Gupta, India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and theCalifornia Consumer Privacy Act of 2018,37 Berkeley J.Int'lL.481 (2019).

[334]Sougata Talukdar, *Privacy and Its Protection in Informative Technological Compass in India*, 12 NUJS L. Rev. 1 (2019).

This section shall deal with the existingprovisionsof the Act inorder to analyze the existing framework for data protection in India.

The ITActadoptsa conventional e-commerce-orienteddefinitionoftheterm"data" under its scheme. The emphasis on computer and other forms of memory storages implies the initial legislative intent behind the provision. It should also be noted that the restricted meaning of term data has undergone considerable changes in the wake of subsequent provisions[335].

> *"(o) 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner,andisintendedtobeprocessed,isbeingprocessedorhasbeenprocessed in a computer system or computer network, and may be in any form (including computer printouts magnet ic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer[336]."*

The scope of the IT Act appears to be confined to the e-commerce activities and the prime focus of the definition of data in the Indian law was to further the cause of internet governance in the information technology sector. This proposition may be appreciated from the fact that the concept of data protection was far away from the Indian conception of privacy and informational self-determination. The fact that there is any law in existence in India can be attributed to the subsequent amendments[337] that were brought in the IT Act. The two most notable pillars of the data protection scheme in the country are Section 43A and Section 72A of the Act.

TheschemeofdataprotectioninIndiacanbebroadlyclassifiedundertwocategories, viz.the Cyber Contraventions and the Cyber offences.While, the Cyber

[335] *Id.*

[336] THEINFORMATIONTECHNOLOGYACT,2000.2(0).

[337] LathaR.Nair,*DataProtectionEffortsinIndia:BlindLeadingtheBlind*,4IndianJ.L.&Tech.19 (2008).

Contraventions, are in the nature of civil wrongs the Cyber offences, as the name suggests are more severe in nature and attract penal consequences. The first post for an insight into the provisions of a statutory law in India saw its dawn in the form of Section 43 A of the IT Act and the provision seeks to impose a liability upon the companies that fail to process the data in a negligent manner without taking reasonable safeguards and security procedures.[338] Violations of the provisions of the section falls within the ambit of cyber contravention. The term contravention is notably very restricted in its extent and it includes all the unwarranted inference in theinformationalprivacyoftheindividualthroughanunauthorizedintrusionintothe data stored in computer or computer network[339].

The bulwark of codified Indian data protection law lies in the Chapter IX of the IT Act. The Section 43 of the Information Technology Act, 2000 provides for the liability of the data controller in case there is a breach

43ACompensation forfailureto protect data. -Where abody corporate, possessing, dealingorhandlinganysensitivepersonaldataorinformationinacomputerresource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by wayofcompensationtothepersonsoaffected.Explanation.-Forthepurposesofthis section, -

(i) "bodycorporate"meansanycompanyand includesafirm,soleproprietorshipor other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and proceduresdesignedtoprotectsuchinformationfromunauthorisedaccess,damage, use,modification,disclosureorimpairment,asmaybespecifiedinanagreement

[338]AsangWankhede,*DataProtectioninIndiaandtheEU:InsightsinRecentTrendsandIssuesinthe Protection of Personal Data*, 2 Eur. Data Prot. L. Rev. 70 (2016).

[339]Wilson,B.,2010.DataPrivacyinIndia:TheInformationTechnologyAct. *SSRNElectronic Journal.*

betweenthepartiesorasmaybespecifiedinanylawforthetimebeinginforceand in theabsenceofsuch agreement or any law, such reasonablesecurity practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitivepersonaldataorinformation"meanssuchpersonalinformationasmay be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit[340].

Asimplicitfromthetextoftheprovision,theSectionpurportstoimposepenaltiesupon those body corporates dealing, possessing and handling the sensitive data and fail to maintain and implement reasonable security measures and as a result of which there is awrongfulgainorawrongfullosstoaperson,thesaidbodycorporateshallbeliableto paydamagestotheaffectedperson.Themeaningofwrongfulgainhastobeconstrued in accordance with the definition in the Indian Penal Code.

Ascanbeinferredfromthebarereadingofthesection,theliabilitieswillariseoutonly againstthebodycorporates,thatistosay companies,corporations,proprietorshipsand the other sections of group of individuals. The exemption of the individuals from the fangs of the penal provision does suggest that the intention of the legislature behind enacting the said section was primarily to the body corporates dealing with processing ofpersonaldata.However,intheviewoftheauthorthescopeandambitoftheprovision is immensely limited and the following are the pre conditions that must be satisfied in order to attract the penal provisions.

- TheData inpossessionmustbeofsensitive character
- The Computer resource processing the data must be owned and run by a body corporate.
- The body corporate must not be negligent in handling the data and there must be a lack of reasonable security standard.

[340]THEINFORMATIONTECHNOLOGYACT,200043A

- Most importantly, such negligence must have resulted inwrongful gain or wrongful loss.

Apart from the very restrictive provision that seeks to protect the breaches of informationalprivacyinthenon-contractualrelations,theIndianlegislaturein2009, through an amendment introduced section 74 A of the Information Technology Act to protect the privacy under the contractual relations.

The IT (Amendment) Act, 2008 (ITAA 2008), introduced in the aftermath of the 26/11 Mumbai attacks has established a strong data protection regime in India. It addresses industry'sconcernson data protection, and creates amorepredictivelegal environment for the growth of e-commerce that includes data protection and cyber-crimesmeasures,amongothers.Sensitivepersonalinformationofconsumers,heldin digitalenvironment,isrequiredtobeprotectedthroughreasonablesecuritypractices by the corporates. Additionally, ITAA 2008 made it obligatory for them to protect dataunderlawfulcontractsbyprovidingforpenaltyforbreachofconfidentialityand privacy.

4.3 Information Technology (Reasonable Security Practices and Procedures and Sensitive Person Data or Information) Rules, 2011

As implicit from the provisions of the Information Technology Act, 2000, the definition of the sensitive personal data was nowhere provided, leaving out a wide roomforconfusionandinstancesofmisinterpretation[341].Thesection43AoftheAct providesfortheframingofnewrulesfromtimetotimeandinexerciseofthispower, the Ministry ofCommunications and Information Technology in 2011 came up with the "Information technology (Reasonable Security Practices and Procedures and SensitivePersonDataorInformation)Rules,2011".Itwouldbeoptimumforour

[341] Information technology (Reasonable Security Practices andProcedures and Sensitive Person Data or Information) Rules, 2011, Rule 03.

analysis to have a glance at some of the relevant parts of the rule to have a holistic view of the existing data protection regime in India.

While the rules, do leave a major chunk of the definitions of the IT Act, 2000 unaltered, they do fill some of the major loopholes of the Act and thus seek to chalk outaworkablepieceofdataprotectionlegislationthatisconducivetotheprotection ofinformationalprivacyofthecitizens.OneofthemostnotableadditionsoftheRules is the definition of the Sensitive Data.

The Rule is quite widely worded and does take into its fold almost all the data that can have a direct bearing upon the right to privacy of an individual in case it gets leaked. However, the proviso to the rule does exclude the data already in public domain from the ambit of the definition of sensitive data.

Therequirementtoobtaintheconsentoftheprovideroftheseensitivedatadoes embody the necessity of element of consent for processing the data. Further the rule specifies that the data shall be collected only for the purpose sanctioned by the law. These rules further recognize the established principles of data protection including therighttopurposelimitation[342],therighttofairnessinprocessing[343]andtheprinciple of time limitation[344]. In addition to these principles, the rules also require the body corporatescollectingsensitiveinformationtohavearobustprivacypolicy[345]andtake adequate measures to afford safety to the personal sensitive data of the individuals. However,therulesprovideafreepasstothegovernmenttosendalltheprinciplesof dataprotectiononatossandallowthegovernmentandthelawenforcement authoritiestoaccessthesensitivepersonaldataoftheindividualswithouttheir

[342] Information technology (Reasonable Security Practices andProcedures and Sensitive Person Data or Information) Rules, 2011, Rule 04.
[343] Information technology (Reasonable Security Practices andProcedures and Sensitive Person Data or Information) Rules, 2011, Rule 04.
[344]Information technology (Reasonable Security Practices and Procedures and Sensitive Person Data or Information) Rules, 2011, Rule 04
[345] Information technology (Reasonable Security Practices andProcedures and Sensitive Person Data or Information) Rules, 2011, Rule 04

consent. Moreover, the adjudicating body Cyber Appellate Tribunal is appointed by the central government[346]. With no independent adjudicating body in place and no shield against the possible intrusions into the right to privacy by the government, a robust data protection regime in India remains a distant dream.

4.4 Privacy in the Health Sector

Therecanbenodenialtothefactthattheinformationrelatedtothehealthandmedical history of the citizens do form an inherent aspect of the right to privacy. It has been repeatedlyheldbytheConstitutionalCourtsinIndiaandabroadthatthedisclosureof themedicaldetailscouldleadtoanunwarrantedinvasionintothepersonaldomainof theindividualstherebycausingextremedisturbancestothetranquilityoftheperson. The Supreme Court while highlighting the importance of the information self-determination in the matters concerning the medical history, in Mr. X v Hospital Z held that:

> *"Right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political. As already discussed above, Doctor-patient relationship, though basicallycommercial,is,professionally,amatterofconfidence:and,there- fore, Doctors are morally and ethically bound to maintain confidentiality. Insuchasituation,publicdisclosureofeven trueprivatefactsmayamount toaninvasionoftheRightofPrivacywhichmaysometimesleadtotheclash of one person's "right to be let alone" with another person's right to be informed. Disclosure of even true private facts has the tenancy to disturb a person's tranquility. It may generate many complexes in him and may even leadtopsychologicalproblems.Hemay,thereafter,haveadisturbedlifeall through"*[347].

[346] Information technology (Reasonable Security Practices and Procedures and Sensitive Person Data or Information) Rules, 2011, Rule 04

[347]Mr.Xv.HospitalZ.AIR1999SC495

This binding precedent of the Hon'ble Supreme Court, in the clearest of terms lays down the rule that even the true information about the medical history of a patient can't be disclosed without their consent. Even the SPDI Rules, 2011 categorize the health-related information as sensitive data and hence prescribe that these data can't be disclosed to a third party without their consent. However, to the contrary, the Clinical Establishment Rules, 2012 mandate the hospitals to maintain an electronic recordofthemedical historyofthepatients[348].However,dueto thenon-application of the rules on the public bodies, the Hospitals run by the governments are exempt from any of these rules and thus provide name-sake of protection from the unwarranted intrusions in the right to privacy of the citizens.

4.5 Existing Surveillance Regime in India

ThemostcrucialaspectoftheupcomingdataprotectionlawinIndiaisthelimitsthat it seeks to imposeupon thescopeand width oftheright to privacy. Thelawbeing at a very nascent stage in the field, it is imperative that it shall take a few years for the courts to come up with a settled approach in order to gauge the extent to which the right to privacy can be exercised. The judgment in Puttaswamy, for sure is going to set in motion a regime that will secure data privacy of billions of Indians to a great extent.ItwouldbewrongtopresumethatPuttaswamyistheendofthe endeavourof securing data privacy of the citizens, instead it's the beginning. At This juncture we are concerned with the what the Court held in Puttaswamy and how did it justify it and how shall the upcoming data protection regime in India be influenced by it.

It may be noted that the prime cause of contention between the petitioners and the respondentsinPuttaswamywasrelatedtothenatureofrighttoprivacy.Whetherthe righttoprivacyisanabsoluteoneordoesitcomewithinherentlimitations?Andifit isn't absolute, what are the imitations and how does the court justify them? The law onthe subject is atquiteanascent stagebutthePuttaswamy does provide a template

[348]See,ClinicalEstablishmentRules,2012

todeterminethesituationsinwhichthebreachofprivacybythestatecanbejustified.

Through the course of our discussion in the following sections we shall seek to explore the nuances of the limitations placed by the SC on the right to privacy. This is the most important part of the issue at hand as the government is likely to accept that citizens have the fundamental right to privacy yet it shall certainly look for alternatives to justify its interference in the private domain of the individuals. The Data Protection Bill, 2019 has been sent to the select committee which is highly unlikely to alter the "exemptions" clause in the proposed bill.

4.5.1 Privacy and Surveillance

The greatest inhibition to the recognition of right to privacy in Indian constitutional schemeistheabsenceofexpressorevenanimpliedmentionofprivacyintextofthe constitution or the constituent assembly debates. It is only through a functional and structural interpretation of the provisions of the constitution that the courts in India have been able to locate the right to privacy within the constitution. However, unsurprisingly, it has taken over six decades for the Indian courts to recognize the place of individual at the core of right to privacy.

"[i]fIndiadoesn'twanttolooklikeanauthoritarianregime,itneedstobetransparent about who will be authorized to collect data, what data will be collected, how it will be used, and how the right to privacy will be protected[349].

Unfortunately, the upcoming data protection regime does exactly what it must have not done by giving a free hand to the enforcement agencies to encroach upon the personal data of the individuals.

Theonlysourceofguidance(readasmisguidance)totheIndiancourtsalltheseyears wasrootedinthespacebasedunderstandingoftherighttoprivacyunderthefourth

[349] AddisonLitton,TheStateofSurveillanceinIndia:TheCentralMonitoringSystem'sChillingEffect on Self-Expression, 14 Wash. U. Global Stud. L. Rev. 799 (2015).

amendment and the fact that the constituent assembly had summarily rejected the inclusionofanysuchprotectionintheconstitutionofIndia,playedadecisiverolein shapingthedataprotectionregimeinIndiaforyears[350].ThefirstcasewhereintheSC had the occasion to examine the existence of right to privacy within the meaning of right to property was *M. P. Sharma and Others vs Satish Chandra*[351]. In order to examinethevalidityofstate'sincursionanditsadoptionundertheIndianschemethe SC referred to several judgments of the American Supreme Court to hold While rejectingtheadoptionofSpatialprivacyincontextofsearchandseizurebythestate., the court held that:

> *"A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to Constitutional limitations by recognition of a fundamentalrighttoprivacy,analogoustotheAmericanFourthAmendment,we havenojustificationtoimportit,intoatotallydifferentfundamentalrightbysome process of strained construction*[352]*."*

Thus,itmaybeobservedthatthecourtrefusedtoadoptthefourthamendmentdirectly within the constitutional scheme on two grounds. First, it relied on the originalist interpretationandsimplyrefusedtoreadthefourthamendmentintotheIndianscheme forthereasonthatithadbeenomittedbytheconstituentassembly.Thesecondreason was more of justification based on the premise that the state had a finding overridingpowerofsearchandseizureforensuringthesocialsecurity.However,this propositionwasshortlivedandshortlythereafterin*KharaksinghvStateofUP*[353]the SC came up with an entirely different interpretation of the ambit of the right to privacy.Inthiscase,theissueconcernedanadministrativeorderthatsoughttoconfer

[350]DhirajR.Duraiswami,*PrivacyandDataProtectioninIndia*,6J.L.&CyberWarfare166(2017).
[351]M.P.SharmaAndOthersvsSatishChandra,1954AIR 300
[352]*Id.*
[353]KharakSinghvsTheStateOfU.P.&Others,1963AIR1295

the powers of search and seizures upon the police officers on the houses of history sheeters.Thisbeinganexecutiveorderwouldnotfallwithinthemeaningoflawunder Article 13 of the Constitution, nonetheless the court went on to examine the validity ofsuchrestrictiononthepremiseofArticle21oftheconstitution.Drawinginferences from the word "dignity" mentioned in the preamble, the SC noted that an unreasonableinvasionintothehomeofanindividualwoulddeprivehimofthemental peace and dignity. Although the court refused to read the right to privacy as one of thefundamentalrightsguaranteedundertheconstitution,itvirtuallyendorsedthefact that tracking the movements of the persons does actually violate the privacy.On a different axle, Justice Subba Rao drew a correlation between personal liberty and seclusion and held that:

> *"It is true our Constitution does not expressly declare a right to privacy as a fundamentalright,butthesaidrightisanessentialingredientofpersonalliberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where lie lives with his family, is his "castle": it is his rampart against encroachment on his personal liberty"*[354].

It must be noted that the Justice Subba Rao in his dissenting opinion, showed exemplary feat of Judicial creativity by reading the right to privacy in not only right tolifeandlibertybutArticle19aswell.Emphasizingonthewordfreely,heobserved, "*befreefromrestrictionsorencroachmentsonhisperson,whetherthoserestrictions or encroachments are directly imposed or indirectly brought about by calculated measures*[355]."

He refused to exclude the element of privacy from the freedom of speech and expression while rejecting the notion that the freedom of expression is an abstract concept devoid of any psychological underpinnings:

[354]KharakSinghvsTheStateOfU.P.&Others,1963AIR1295,1294.
[355]KharakSinghvsTheStateOfU.P.&Others,1963AIR1295,1301.

"Assuming thatArt. 19 (1) (d)of the Constitution must be confined only to physical movements, its combination with the freedom of speech and expression leads to the conclusion we have arrived at. The act of surveillance is certainly a restriction on the said freedom. It cannot be suggested that the said freedom is also bereft of its subjective or psychological content, but will sustain only the mechanics of speech and expression[356]".

It may be argued that *Kharak Singh* marked the half-hearted endorsement of the "individual"based conception ofright to privacy. It maybe argued that this casedid highlight some of the most pressing concerns regarding the state of present-day surveillance regime in India. Before revisiting the issues that overlap in the present scenario and those addressed/unaddressed by the court in *Kharak Singh*, a brief analysisofthecasesthatfollowedisnecessarytointercepttheattributesofthepresent surveillance regime in India.

ThetelephonicconversationofaninnocentcitizenwillbeprotectedbyCourtsagainst wrongful or high handed' interference by tapping the conversation. The protection is not for the guilty. It must not be understood that the Courts will tolerate safeguards for the protection of the citizen to be imperilled by permitting the police to proceed byunlawfulorirregularmethods.Inthepresentcasethereisnounlawfulorirregular method in obtaining the tape recording of the conversation.

He said that although it is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the right is an essential ingredient of personal liberty, that in the last resort, a person's house where he lives with his family, is his castle that nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy and that all the acts of surveillance

[356]KharakSinghvsTheStateOfU.P.&Others,1963AIR1295,1301.

Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, that fundamental right must be subject to restriction on the basis of compelling public interest.

InwhathasbeenwidelytermedasoneofthemostnotablejudgmentsoftheSupreme Court against the surveillance regime in India, the SC in *People's Union for Civil Liberties (PUCL) v. Union of India*[357], the question under challenge, although not directly was section 5(2) of the Indian telegraph Act, that has been the most used weapon of the government in its surveillance regime.

Itmaybepointedoutthattheprovisioncompletelyendorsedthefactthattheeventhe minutestdetailsrelatingtothemedicalhistoryofanindividualmaybedetrimentalto the dignity of the individual and hence must be conferred greater protection. At this juncture, the judgment in Mr. X v Hospital Z[358], where the SC had observed that the provision has been acknowledged in letter and spirit where in the SC had noted that,

> "*privatefactsmayamounttoaninvasionoftheRightofPrivacywhich maysometimesleadtotheclashofoneperson's"righttobeletalone" with another person's right to be informed. Disclosure of even true private facts has the tenancy to disturb a person's tranquility. It may generate many complexes in him and may even lead to psychological problems*[359].

The Bombay High Court in 2019 was presented with the opportunity to adjudicate upon the law pertaining to phone tapping and surveillance in the post-Puttaswamy era, applyingtheprinciplesinrelationtotheright toprivacytosection5(2)oftheIT Act.

The HighCourtinthe*VinitKumar*[360]Case,inthequestionofinterception,held:An

[357]People'sUnionforCivilLiberties(PUCL)v.UnionofIndia,(1997)1SCC301.

[358]Mr.Xv.HospitalZ, AIR1999**SC**495.

[359]*Id.*

[360]2019SCCOnLineSC1380.

order of interception under section 5(2) of the IT Act can only be given in situations of 'public emergency' or 'public safety'. If interception has been undertaken in contravention of Section 5(2) of the IT Act, it is mandatory for the said intercepted messages to be destroyed.

As per the BN Srikrishna committee report, "*the Surveillance should not be carried outwithoutadegreeoftransparencythatcanpassthemusterofthePuttaswamytest ofnecessity,proportionalityandddueprocess.Thiscantakevariousforms,including informationprovidedtothepublic,legislativeoversight,executiveandadministrative oversightandjudicialoversight*[361]*."*Thereportexplicitlymentionedtheneedforthe state to adhere to the principles laid down in the Puttaswamy judgment for the purposes related to surveillance. In this section, we shall first discuss in detail the principlesthat werelaid downbythe IndianSupremeCourt whichmustbefollowed whiledepriving apersonoftheirfundamentalright.Righttoprivacybeinganintrinsic aspect of right to lifeand libertyas recognized in Puttaswamy is a fundamental right and hence the exemptions granted to the state agencies where these constitutional safeguards don't apply need to fulfill the tests identified under the judgment. The Courts in India have traditionally been using different tests for determining the parameterstoconfinetherightsofthecitizens.Therearethreedifferenttestsbythe Supreme Court has evolved over time to check whether the curtailment of fundamental rights can bejustified. In orderto analyzewhethertheprovisions under thepresentbillthatseektoexempttheagenciesfromtheapplicationoftheprotections provided under the Act, will pass muster the tests laid down in binding judicial precedents, we shall now have a brief overview of these tests.

In majority judgment in Puttaswamy adopted a unique version of meaning of the proportionality testtoapplyintheIndianconstitutional scheme.Fordetermining the extentofprivacyinfractions,thecourtsinIndiawillfollowthedoctrineof

[361] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (Accessed on 12th Dec. 2019).

proportionality in the upcoming days and the constitutionality of the provisions providing for exceptions under the data protection bill will be anchored around the test.The doctrine of proportionality as applied in different jurisdictions across the worldisn'texactlythesameastheonethatwasunderstoodbythehonorablejudges in Puttaswamy. However, it must be acknowledged that the judges did an elaborate study of the contours of the test before altering the existing tests for infringement of privacy.

The Constitutional courts in Germany have adopted a three-pronged test in order to ascertainthevalidityofanyprivacy infringement. Thefirst facetofthetest concerns with the legitimacy of the goal for which the step is being taken. The second facet requires that there must be a rational nexus between the means and the goal that is sought to be achieved. The third facet requires that there shouldn't be any equally officious alternative that is less restrictive in nature to achieve the goal, this is also describedasthenecessitystage.Thelaststageisthe"balancingstage"whichrequires that the measurebeing taken by the state must nothaveadisproportionate impact on therightsofthecitizens.WhilequotingthestanzafromProf.Bilchitz'sthesistheSC hasexplainedthatwhileassessingthedeterminativestepofnecessity,thecourtmust first of all identify all the possible alternatives to the policy adopted by the government and then proceed towards examining the issue whether these measures could be an effective alternative.If the alternative and less restrictive policy can achieve the objective sought to be achieved by the government in a real and substantial manner, it should be preferred.

4.6 How will the Doctrine of Proportionality be applied in India?

As per the ratio of Puttaswamy, the courts will apply the following standards to determine the constitutionality of the provisions.

- IstheStatepursuinganaimwhichislegitimate?Hereasonemaynotice,theaim oughtnotbeacompellingoneandifthecourtsfindthattherestrictionsaresought tobeimposedtomeetalegitimateaimthenthefirstfacetoftestshallpassmuster.
- Is the State using reasonable means to achieve the legitimate aim and is there a nexus between the aims and the objective? The second fulcrum of the tests shall lieuponthereasonablenessofthemeans.Ifthemeansadoptedbythestate,inthe view of the courts, are not reasonable, the test shall fail.
- The third question involves an enquiry into an equally effective alternative method that could beresorted to forachieving the sameends whilehaving lesser intrusion upon the rights of the citizens. For doing so the courts will go into the following aspects of the subject.

a) *Look for the alternative measures that are equally effective in achieving the legitimate aim sought to be achieved by the state*
b) *Are these measures taken up by the state really necessary and effective for achieving the objective?*
c) *Ifthefirsttwoconditionsaresatisfied,whatwillbetheimpactoftheserestrictions on the rights of the citizens?*
d) *At this juncture, the court shall use the relevant circumstances to perform the balancing exercise*.

- The balancing exercise is done by the courts to check whether the intrusion into the right and the importance of the right are proportionate to each other or not. Since, the test has been applied only once in the Indian domain in Puttaswamy, wewouldgetaclearerpictureoftheparametersthatthecourtusestothisexercise in the coming years.

In Pursuance of Legitimate Aim: We shall refer to the application of the facets of proportionality in Puttaswamy with respect to Aadhar to analyze whether the provisions in the draft bill, that provide the central government with wide powers of exemption of the agencies from the operation of the Act, shall pass the tests or not. Thefirsttestconcernswithlegitimacyoftheaimthatthestatewishestopurport.The precedentinPuttaswamycanbetakenasayardsticktotestthevalidityofthesections

in the data protection bill that aim to promoting the ends of social justice will fall within the domain of legitimate sate interest within the constitutional scheme. The majority in Puttaswamy had noted that[362]

> *"Section 7 of theAadhaar Act is aimed at offering subsidies,benefits or services to the marginalised section of the society for whom such welfare schemes have beenformulatedfromtimetotime.Thatalsobecomesanaspectofsocialjustice, which is the obligation of the State stipulated in Para IV of the Constitution. The rationale behind Section 7 lies in ensuring targeted delivery of services, benefits and subsidies which are funded from the Consolidated Fund of India".*

The processing of data without the consent of data principal under the provisions of proposed bill that are aimed at furthering the cause of social justice, allotting the subsidiesandpromotingwelfareschemesofthestatewilllikelyfallwithintheambit of legitimate state interest and hence will pass constitutional muster.

This view was expressly endorsed in Puttaswamy where, the majority affirmed that that, *in a welfare State, where measures are taken to ameliorate the sufferings of the downtrodden, the aim of the Act is to ensure that these benefits actually reach the populaceforwhomtheyaremeant.ThisisnaturallyalegitimateStateaim*[363].Hence, as far as the first facet of the proportionality test is concerned the provisions of the proposed bill that's eek to process the personal data without the consent of data principal will be satisfied.

TheNexusTest:Thesecondlimboftheproportionalitytestrequiresarationalnexus between the means and the object sought to achieved. The judicial interpretation of this facet of the test is quite settled and the majority in Puttaswamyreteriaeted the established test while holding that:

[362]KSPuttaswamyv.UnionofIndia,(2019)01SCC01, 376.
[363]KSPuttaswamyv.UnionofIndia,(2019)01SCC01, 378.

"There must be a direct and proximate nexus or reasonable connection between the restrictions imposed and the object sought to be achieved. If there is a direct nexus between the restrictions, and the object of the Act, then a strong presumption in favour of the constitutionality of the Act will naturally arise[364]*."*

Baseduponthesameprinciple,themajorityupheldthevalidityofAadharandnoted, "*We have already held that it has substantial nexus with the appropriation of funds fromtheConsolidatedFundofIndiaandisdirectlyconnectedwithArticle110ofthe Constitution*[365]".Baseduponthislineofreasoningtheprovisionsenshrinedunderthe proposeddataprotectionbillshallpresumablypassthesecondfacetofthetestaswell. The processing of data without the consent of the data principal, when there is a legitimate aim to be achieved by the state and such aim requires the processing of data, the provision shall pass the requirement of "nexus test".

The third and the most important facet of the proportionality test is the existence of necessityandtheexistenceofequallyeffectivebutlessrestrictivemeasurestoachieve thelegitimateaimthatissoughttobeachieved.Weshallanalyzetheprovisionsunder theexemptionclausesunderthisprongtotestwhetherthenecessityofproportionality is met or not. The test of "necessity" is the most important aspect of the third prong ofproportionalitytest;however,thecourtseemstoignoretherelevanceofthisaspect of the test. While upholding the German notion of doctrine of proportionality, the courtholdsthatthereisalwaysapossibilitythatanalternativewillnotbeaseffective as the one that is being adopted by the government while being less intrusive. The courtendorsesthefactthat,"*almostallpoliciesarenecessarybecauseanyalternative policywillusuallyhavesomedisadvantagewhichmeansthatitcannotbeconsidered equally effective*."

Itissubmittedthatitisunfortunatethatthecourtwentaheadwiththeassumptionthat therecan'tbeanequallyefficientalternativesubstitute.Followingthesamelineof

[364]KSPuttaswamyv.UnionofIndia,(2019)01SCC01, 548.
[365]KSPuttaswamyv.UnionofIndia,(2019)01SCC01, 458.

reasoning,itupheldthevalidityofsection7ofAadharActwithoutevenconsidering the other options

> *"Insofarasthirdcomponentisconcerned,mostofitstandsansweredwhileinthe discussion that has ensued in respect of component No. 1 and 2. The manner in which malpractices have been committed in the past leaves us to hold that apart from the system of unique identity in Aadhaar and authentication of the real beneficiaries, there is no alternative measure with lesser degree of limitation which can achieve the same purpose. In fact, on repeated query by this Court, even the petitioners could not suggest any such method[366]"*

It is further submitted that the courts inability to appreciate the relevance of this part ofthetestleavesagreatloopholeinthepursuitofprotectionoffundamentalrightsof the citizens. As, is quite apparent from the wide window under the proposed data protectionbill,thegovernmentwilleasilygetawaywiththeargumentthattherecan't be an equally effective method to achieve the legitimate aim and it will always have the observation in the judgment to justify disregard for an alternative method.

It maybepointed out that theright formulationofthis aspect ofthetest requires that theCourtmustassessthepossibilityofalternativesthatmaybeappliedforachieving the same aim. When the court does get the list alternatives that may be applied to achievethatlegitimateaim,itshouldgoontoconsiderwhetherthesemethodswould substantially fulfill the objectives that the state seeks to attain through the impugned act.Instead,ofmeasuringtwodifferentactsonagoldenscale,thecourtsmustassess whether the alternative method will in pith and substance fulfill the legitimate aim that the state seeks to pursue. Unfortunately, the majority in Puttaswamy failed to apply any of the test in its true spirit and thus left a great lacuna in preserving the privacy infringements of the citizens.

[366]KSPuttaswamyv.UnionofIndia,(2019)01SCC01,382.

Necessity: The most controversial aspect of the proposed bill that provides for the wide range of exceptions under the proposed data protection bill, 2019to the central government agencies[367].

An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionatetothelegitimateaimpursuedandifthereasonsadducedbythenational authoritiestojustifyitare"relevantandsufficient.Theprotectionofpersonaldatais of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.

The bill does away with the necessity of consent and notice for the processing of personal data by a sweeping assertion that, "*The provisions of sub-section (1) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12*[368]*."*As a result, the necessity of giving the notice to the data principal in the cases wherein their data is being processed without their consenthasbeendoneawaywith.Thisisasubstantialdeparturefromtheprovisions ofthepreviousdraftbill,whichmandatedtheissuanceofnoticetothedataprincipals in cases of non-consensual processing of data. The draft bill had curtailed the scope of non-consensual processing of personal data without giving notice to the data principal medical emergency, breakdown of public order and natural disaster[369]. However, the bill in its present form incorporates every element of section 12 in the domainof"*uninformednon-consensual*"processingofpersonaldataandthus

[367]ThePersonalData ProtectionBill,§ 35, *supra*note47.WheretheCentralGovernmentissatisfied thatitisnecessaryorexpedient,—(i)intheinterestofsovereigntyandintegrityofIndia,thesecurity of the State, friendly relationswith foreign States, public order; or(ii) for preventing incitement to thecommissionofanycognizableoffencerelatingtosovereigntyandintegrityofIndia,thesecurity of the State, friendly relations with foreign States, public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subjecttosuchprocedure,safeguardsandoversightmechanismtobefollowedbytheagency,asmay be prescribed.

[368]ThePersonalDataProtectionBill,2019,§7(3),*supra*note 47.

[369]ThePersonalDataProtectionBill,2018,§15,DraftBill,2018(India).

broadenstheambitofprocessingwithoutobtainingtheconsentofthedataprincipals. Itmaybeinferredthatsuchwidewindowsfornon-consensualprocessingofpersonal data goes against the very foundation of informational self-determination.

This goes on to imply that, for the purposes of processing of personal data without the consent of the data owner, on the hugely extensive grounds enumerated under section12,theprocessorwillnotbeboundtoinformthedataowneraboutanyaspect of the processing of personal data, if the result of notice would amount to frustration of the purpose for which the data is sought to be processed.[370] It must also be noted that the proposed section uses the term, "*prejudices*" the purpose for which data is beingprocessedundersection12,insteadofthetern,"*frustration.*"Thiswouldimply that even an apprehension of a minor deviation from the objective behind the processing of personal data will allow the data fiduciaries from complying with the requirement of notice for non-consensual processing of data.

Itissubmittedthattheprovisionthataffordsahugewindowtothedataprocessorsto denytherightofthedataprincipalstobeinformedaboutthepurposeforwhichtheir dataisbeingprocessed,bywhomistheirdatabeingprocessedandeveryotheraspect related to processing of data. The provision seeks to push all the principles of data protection into abeyance by creating a regime that could secretly process one's data without even affording them a right to know anything related to the processing of their own data. These provisions if manage to escape the scrutiny of the joint committee,shallflyinthefaceoftheconceptof"informedconsent"andprecludethe billions of Indians from the right to an informed consent. The provision shall be instrumental in laying the foundation of a state sponsored surveillance module, wherein the data of the individuals will be processed without their consent and without them even knowing that their data has been processed. This shall bring into theframeahugeamountofopacityandvaguenessintheoperationsofdatafiduciary.

[370] JOHN KLEINIG, THE NATURE OF CONSENT IN THE ETHICS OF CONSENT - THEORY AND PRACTICE 109-112 (1st ed. 2009).

It is submitted that the provision tilts the pendulum of convenience in the favor of data fiduciaries.

It is an established legal principle that the consent can't be free at all when the one whohasgivenis,isunabletowithdrawitwithoutanydetrimenttohisinterests[371].To put it more plainly, the withdrawal of consent has to be as easy as the furnishing the consent had been[372]. However, the Personal Data Protection Bill 2019, like the previousdraftBill,does continuetofrownuponthewithdrawalofconsent.While,it adopts, in letter, the principle that "*the ease of such withdrawal comparable to the ease with which consent may be given*" but fails to honor the spirit of the principle. The section 11(6) of the Data Protection Bill, 2019 goes on to lay that the in cases where the data principal who has previously given his consent for processing of personaldata,withdrawshisconsentlater, withoutany"validreason"then hewould be liable for all the "*legal consequences for the effects of such withdrawal[373]."*

A close look at the operative part of the order in Puttaswamy signifies that the Court hasseparatelypointedoutthattherighttoprivacy,isaprotected"*asanintrinsicpart oftherighttolifeandpersonalliberty****underArticle21****andasapartofthefreedoms guaranteed by Part III of the Constitution".* The insistence upon right to life and liberty goes on to show that the court expects a greater degree of adherence and insistenceuponstricterstandardsforgrantingtheirviolations.Thisgoesontosuggest thatthecourtconsiderstherighttoprivacytobeonagreaterpedestalascomparedto otherrightsrecognizedbythepartIIIoftheconstitution.Weshallseparatelyconsider righttoprivacyasapartoftherightsrecognizedbythepartIIIoftheconstitutionand as a part of right to life and liberty as enshrined under article 21 of the constitution.

[371]ViktorMayer-Schonberger&YannPadova,*RegimeChange:EnablingBigDatathroughEurope's New Data Protection Regulation*, 17 Colum. Sci. & Tech. L. Rev. 315 (2016).

[372]GeneralDataProtectionRegulation,Recital42(EU2016);ModernizedConvention108, ExplanatoryReport¶42(EU2018).

[373]ThePersonalDataProtectionBill,§11(6), *supra*note47.

Thisrightissubject toreasonable regulationsmadebytheState toprotectlegitimate Stateinterestsorpublicinterest.However,whenitcomestorestrictionsonthisright, thedrill ofvarious Articlesto which theright relates must bescrupulously followed. EachofthetestsevolvedbythisCourt,qualegislationorexecutiveaction, underArticle 21read withArticle 14;orArticle 21read withArticle 19(1)(a)in the aforesaidexamplesmustbemetinorderthatStateactionpassmuster.Intheultimate analysis, the balancing act that is to be carried out between individual, societal and State interests must be left to the training and expertise of the judicial mind[374].

4.7 Righ to Privacy and the Constitution of India

Indianmodelofconstitutionalismhasitjudiciaryatitsfocalpointandthusitbecomes extremelyvitaltoassesstheapproachoftheIndianconstitutionalcourtswithregards to the right to privacy so as to address some of the normative aspects of the interpretation of the proposed Data Protection Law in India. The preamble of Indian ConstitutionistheMagnaCartaofournation,itrepresentsthesocialcontractbetween wethepeopleandthestate[375].It'sequallytruethatthetextiftheconstitutionofIndia doesn'texpresslyorevenincidentallyrecognizetherighttoprivacyasafundamental rightbuthowlongcanthejudiciarylooktheotherwaywhiletreatingtheconstitution to be cast in rock frame? As per Prof. Upendra Baxi, the constitution represents a socialcontractbetweenthestateandthecitizensandisn'tastaticbutanever-evolving documentandithassome"*manifestthemselvesdifferentlyindifferentages,situations andconditions"*[376].However,ablindrelianceupontheorganicnatureofconstitution has been regarded as instrument of felicitating judicial arbitrariness and hence there isaneedofevolutionofatheorythatisbasedonstructureandtheethosofthe

[374]KSPuttaswamyv.UnionofIndia,(2017)10SCC01,224.,637.

[375]MahendraPalSingh, *TheConstitutionofIndia:AContextualAnalysis*,14 SOCIO- LEGAL REV. 228, 228-241, (2018).

[376]UpendraBaxi,*TheRuleofLawinIndia*,6SUR-INT'LJ.ONHUMRTS.7,11-21(2007)

constitution[377]. Justice Chalemshwar came close to justifying the living constitutionalist approach:

> *"The living constitutionalist approach in my view is preferable despite these criticisms, for two reasons. First, adaptability cannot be equated to lack of disciplineinjudicialreasoning.Second,itisstillthetextoftheconstitutionwhich acquires the requisite interpretative hues and therefore, it is not as if there is violence being perpetrated upon the text if one resorts to the living constitutionalist approach*[378] *".*

While judicial discretion is central to judicial interpretations, such interpretations can't ignore the constitutional ethos and structure. Justice Kaul, in his opinion discussed the nature and charter of the constitutionalist interpretation and observed thattheConstitutionoughttobecontinuouslyupdatedtokeepupwiththepaceofthe social change.[379] It is pertinent to note that the recognition of right to privacy as a facet of right to life and liberty as enshrined under Article 21 of the Constitution furthers and supplements the individual based notion of the fundamental rights.

4.7.1 Privacy as A Natural Right

The significance of the judgment in Puttaswamy increases manifolds when views fromtheperspectiveofthesourceoffundamentalrightsandthedoctrinesthatwould govern the justification of suspension of the fundamental rights. The SC in ADM Jabalpur v. Shivkant Shukla[380] had asserted that, "*Independently of the constitution and the laws of the State, natural rights can have no legal sanction and cannot be enforced*.[381]" In the most notorious judgment which the apex court of any true democracycancomeupwith,theSupremeCourtinADMJabalpurhadhit

[377]H.M.Seervai,Theemergency,futuresafeguardsandthe habeascorpuscase:ACriticism1,3 (1978).
[378]K.SPuttaswamyv.UnionofIndia,(2017)10SCC01, 516.
[379]*Id.*at516.
[380]ADMJabalpurv.ShivkantShukla,(1976)2SCC521.
[381]ADMJabalpurv.ShivkantShukla,(1976)2SCC 52.

unprecedented low in holding that there existed no right outside the constitution[382]. What Puttaswamy did was to recognize that our constitution didn't create the rights but it just recognized their existence[383]. The majority regarded privacy as a natural right to hold that:

"privacyisaconcomitantoftherightoftheindividualtoexercisecontroloverhisor herpersonality.Itfindsanoriginginthenotionthattherearecertainrightswhichare natural to orinherent ina humanbeing. Naturalrights areinalienable becausethey areinseparablefromthehumanpersonality.Thehumanelementinlifeisimpossible to conceive without the existence of natural rights"[384]

Justice Bobde (as he then was) held that privacy as an intimately connected to two values whose protection is a matter of universal moral agreement: the innate dignity andautonomyofman[385].Theotheropinionsalsoendorsetheevolutionofconceptof righttoprivacy and the endorsedthe factthatthedignity-basednotionoftherightto privacy would deny the justiciability of the spatial and the relational notions of the righttoprivacy.Oneofthemostimportaspectsofthejudgmentswastheendorsement of an inherent right to informational privacy as one of the prongs of the right to privacy[386]. It is submitted that recognition ofRight to privacy as afundamental right of which informational privacy is an aspect, which lies at the core of the rationale behind a robust data protection regime in the country.

The 2017 was one of the most remarkable years in the arena of transformative constitutionalism in India wherein the SC shed the shackles of a lot of regressive notions that it had voluntarily allowed to inhibit itselffrom adopting to the changing socialandlegaldynamics.Thethemeofthreejudgments*JusticePutatswamyvUnion*

[382]ManeeshChhibber,35YearsLater:AFormerChiefJusticeofIndiaPleadsGuilty,INDIANEXPRESS, Sept. 16, 2011, http://indianexpress.com/article/.

[383]K.SPuttaswamyv.UnionofIndia,(2017)10SCC01, 364.

[384]K.SPuttaswamyv.UnionofIndia,(2017)10SCC01, 365.

[385]*Id.*at537.

[386]GautamBhatia,RighttoPrivacyIndianConstitutionalLawandPhilosophy,Oct22,2019, https://indconlawphil.wordpress.com/category/privacy/.

of India[387], *Joseph Shine v Union of India*[388] and *Navtej Singh Jauhar v Union of India*[389], are woven round a common thread that endeavors to expand the scope of personal freedom in the fullest extent. For over seven decades the Supreme Court of India had repeatedly ignored the infallibility of right to dignity of the individuals on thepretext of morality and social mores. Themost remarkableof thethreejudgment has to be the privacy judgment[390].

In*JusticePuttaswamyv.UnionofIndia*[391],anine-judgebenchoftheSupremeCourt ofIndiaunanimouslyrecognizedtherighttoprivacyasafundamentalrightunderthe constitutionofIndia.Inwhatmaybetermedasthemostnotablejudgmentsprotection the civil rights on India after the dissent of Justice Khanna in ADM Jabalpur v. ShivkantShuklatheSupremeCourtlaiddownthelawthatwillhaveanimpactonthe constitutional landscape of the country[392]. The implications of the holding are going tobeobservedindataprotectionlawsandeveryotheraspectofthelawthatconcerns the aspects of individual liberty. Be it the right to choice of food, dressing, state surveillance, LGBT rights and domains that are likely to surface with the evolution ofsociety. Intheupcomingsections,thefinderwilldealwiththecontoursofthe ruling which are likely to have an impact on the way the Indian data protection laws are interpreted by the judiciary in the coming years.

4.8 The Approach of Supreme Court on Right to Privacy

In *Govind vStateof MP*[393], whileholding thattheright to privacy is an intrinsicpart ofthefundamentalrights guaranteedbytheconstitution,theSupremeCourtchoseto

[387]K.SPuttaswamyv.UnionofIndia,(2017)10SCC01, 537.
[388]JosephShinev.UnionofIndia,(2019)3SCC39.
[389]NavtejSinghJauharv.UnionofIndia, (2018)10SCC 01.
[390]ShamnadBasheer,SroyonMukherjee &KarthyNair,Section377andtheOrderofNature: Nurturing Indeterminacy in the Law, 2 NUJS L. Rev. 433 (2009).
[391]K.SPuttaswamyv.UnionofIndia,(2017)10SCC01, 537.
[392]KalyaniRamnath,*ADMJabalpur'sAntecedents:PoliticalEmergencies,CivilLiberties,and Arguments from Colonial Continuities in India*, 31 AM. U. INT'L L. REV. 209, 210-211 (2016).
[393]Govindv.StateofMP,(1975)2SCC 148.

restrictthemeaning ofprivacytothespaces andinstitutionswithinthesocietywhile completely omitting the scope of protection of the individuals[394]. The formulations such as marriage, home and motherhood don't go beyond protecting the social relationsandinstitutionsandthusadheretoarestrictiveunderstandingoftherightto privacy[395].Inwhatusedtobeunderstoodastheprivacyathome,thecourtinGovind justified the restricted understanding of the right to privacy with two theories in the backdrop[396].

The first theory that justifies the existence of privacy at the homes is that the acts takingplaceinsidethefourwallsofthehomethatcausenooffensetotheothersaren't constitutional protection able. The second theory which sounds much plausible rests on the proposition that an individual's needs a "sanctuary" that is free from social controlandinterventionwhere"individualscandropthemask.desistforawhilefrom projecting on the world the image they want to be accepted as themselves, an image that may reflect the values of their peers rather than the realities of their natures[397]". ThephasewitnessedadesperateattemptonthepartoftheSupremeCourttocreatea space forthe right to privacy in the Indian constitutional scheme, but of coursein an extremely restricted form.

Oneofthemostnotableobjectionstothehomebasedspatialandrelationalnotionof therighttoprivacyisfoundeduponthearguementthattherighttoprivacystemsfrom the notion that these notions cast a blind eye upon the imbalance of status of relationshipwithinthehome[398].Attimes,therighttoprivacyinhomehasalsobeen

[394] Govind v. State of MP, (1975) 2 SCC 148. The Court emphasized on the social and relational aspectsoftherighttoprivacyandassociateditwithhomewhileobservingthat,"Anyrighttoprivacy must encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation .and child rearing."

[395]Govindv.StateofMP(1975),2SCC148,156.

[396]*Id.*at157.

[397] Alan F. Westin, Privacy and Freedom 33 (1967); Andrew J. McClurg, Kiss and Tell: Protecting Intimate Relationship Privacy through Implied ContractsofConfidentiality, 74 U. Cin. L. Rev. 887 (2006).

[398]MeeraKosambi,GenderReformandCompetingStateControlsoverWomen:TheRakhmabaiCase (1884-1888), (1995) https://doi.org/10.1177/0069966795029001013.

regarded as based upon an understanding that seeks to preserve the male authority within the family[399]. The observations in Govind outline the aspects of the right to privacy.[400]

- The right to privacy is limited to the Spatial boundaries and the activities that it governs are related to the things that are done within the four walls of the home.
- Therighttoprivacyisaimedatpreservingthesocialinstitutionssuchasmarriage and the functions arising out of these institutions[401].
- Decisionalautonomyoftheindividualsthatisbasedonthepremisethat"an individual has the right to take their own decision[402]."

ItookaboldstepfromtheHCofAndhraPradesh,inadecisionthatwaswellahead of its times to break away from the shackles of restrictive interpretation of the right to privacy. Justice Chaudhary in *T Sareetha*[403], entirely premised the understanding of the right to privacy on the right to decisional autonomy and bodily integrity and thus rejected the argument that the site of claim of right to privacy are social institutions and functions arising thereof[404]. The court held that, *"any plausible definition of right to privacy is bound to take human body as its first and most basic referenceforcontroloverpersonalidentity…therighttoprivacybelongstoaperson as an individual and, is not lost by marital association*.[405]" In what may be regarded as the a very radical step, the Court further observed that, "a decree of restitution of conjugal rights thus enforced offends the inviolability of the body and the mind subjected to the decree and offends the integrity of such a person and invades the marital privacy and domestic intimacies of such a person[406].

[399]RuthGavison,FeminismandthePublic/PrivateDistinction,45Stan.L.Rev.1(1992).
[400]Govindv.StateofMP,(1975)2SCC 148.
[401]*Id.*
[402]ThisformulationcanbetracedtothecaseofRoev.Wade,410U.S.113(1973).
[403]TSareethavVenkatasubbaiah,AIR1983AP356.
[404]*Id.*
[405]*Id.*
[406] Ratna Kapur and Brenda Cossman, SUBVERSIVE SITES: FEMINIST ENGAGEMENTS WITH LAW IN INDIA, 123 (1st ed. 1996).

4.8.1 Clashes between spatial, institutional and decisional privacy

The Clashes between the individualistic and institutional conception of right to privacy is most amply reflected by the Courts approach on issues concerning the "offences against marriages" and restitution of conjugal rights. In *T Sareetha v Venkatasubbaiah*[407], the Andhra Pradesh High Court, while giving predominance to theindividualrighttoprivacyovertheinstitutionalprivacy,heldtheSection9ofthe Hindu Marriage Act[408] as unconstitutional on the account of "state interference" in thedecisionmakingofthewomen.However,theDelhiHCregardedtheinstitutional understanding of the right to privacy and held that:

> *"Introduction of Constitutional Law in the home is most inappropriate. It is like introducing a bull in a china shop. It will prove to be a ruthless destroyer of the marriage institution and all that it stands for. In the privacy of the home and the marriedlifeneitherArt.21norArt.14haveanyplace.Inasensitivespherewhich is at once intimate and delicate the introduction of the cold principles of Constitutional Law will have the effect of weakening the marriage bond[409]". Unfortunately, the view taken by the Delhi HC was endorsed by the SC with the much-used reasoning of, "serves a social purpose as an aid to the prevention of break-up of marriage."[410]*

[407] *Id.*

[408] The Hindu Marriage Act, 1955, § 9, No. 25, Acts of Parliament, (India 1955). Section titles as: restitution of conjugal rights, provides that: "When either the husband or the wife has, without reasonable excuse, withdrawn from the society of the other, the aggrieved party may apply, by petition to the district court, for restitution of conjugal rights and the court, on being satisfied of the truth of the statements made in such petition and that there is no legal ground why the application should not be granted, may decree restitution of conjugal rights accordingly."

[409] HarvinderKaurv.HarmanderSingh, AIR1984Delhi66**.**

[410] *Id.*

The view taken in Sareetha can be traced back to the proposition of Justice Brandie inOlmsteadvsNewYorkthatsoughttobalancethepowerbetweenthestateandthe individual in order to secure the right to privacy.[411]

The"Conventionsoffemalechastityandmodesty"haveshieldedwomeninamantle of privacy at a high cost to sexual choice and self-expression.[412] In a considerably maledominatedsocietylikeIndia,thepropositionwouldneednofurtherelaboration and unfortunately, until recently the Supreme Court of India had been proving these apprehensions genuine in the guise of protecting the sanctimony of marriage. It was only in the case of Joseph Shine, that the Supreme Court was able to do away with a substantial chunk of credible criticism surrounding the ill effects of coerced privacy within the home.The SC in Puttaswamy, categorically held accepted the individual basednotionoftherighttoprivacyandallthesixopinionsretreatedtheviewthatthe view that the individual autonomy lies at the core of right to privacy[413]. The speculationregardingtheeffectofrighttoprivacyonthewomenwithinthefourwalls was put to rest by Justice Chandrachud in his opinion, he observes,

> *"Many writers on feminism express concern over the use of privacy as a veneer forpatriarchaldominationandabuseofwomen.Patriarchalnotionsstillprevail in several societies including our own and are used as a shield to violate core constitutional rights of women based on gender and autonomy. Privacymust not be utilised as a cover to conceal and assert patriarchal mindsets. [414]".*

[411] Andrew Jay McClurg, Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places, 73 N.C. L. REV. 989, 999-1002 (1995).

[412] RHONDA COPELON, UNPACKING PATRIARCHY: REPRODUCTION, SEXUALITY, ORIGINALISM, AND CONSTITUTIONAL CHANGE, IN A LESS THAN PERFECT UNION: ALTERNATIVE PERSPECTIVES ON THE U.S. Constitution 303, 314 (Jules Lobel ed., 1988).

[413] K.SPuttaswamyv.UnionofIndia,(2017)10SCC01, 539.

[414] Catherine MacKinnon, Towards a Feminist Theory of the State, (1989). Author adverts to the dangers of privacy when it is used to cover up physical harm done to women by perpetrating their subjection.Yet,itmustalsobenoticedthatwomenhaveaninviolableinterestinprivacy.Privacyis theultimateguaranteeagainstviolationscausedbyprogrammesnotunknowntohistory,suchasstate imposedsterilizationprogrammesormandatorystateimposeddrugtestingforwomen.Thechallenge inthisareaistoenablethestatetotaketheviolationofthedignityofwomeninthedomestic sphere

Justice Chandrachud, it must be mentioned, was most firm in tackling the genuine propositions raised by the feminist thinkers and placing the individual at the core of the right to privacy. With the individual as the basic unit of the constitution, the normative defenses to regressive practices such as marital rape are going to come under the scanner in near future.

4.9 Puttaswamy and the Aftermath

The observation of Justice Chandrachud in Puttaswamy was influential in shedding the non-individualistic notions attached to the concept of privacy in Indian constitutional scheme to a great extent. The first progressive manifestation of the broaderinterpretationofrighttoprivacyisreflectedinJosephShinevUnionofIndia,
wherein the Supreme Court held the regressive adultery law as unconstitutional, defying all the arguments that it had itself stuck to based on the premise of "saving the institution of marriage"[415]. What now represents the current outlook of the supreme court on the concept of privacy is amply reflected in the cases of Joseph Shine v. Union of India and Navtej Singh Jauhar v. Union of India.
As we have noted earlier, the understanding of the notion of right to privacy has undergone` a sea of change over the years. After the landmark judgement in K S Puttaswamy, the commentators had rightly noted that the days of archaic Victorian provisions like section 497 and 377 of the Indian Penal Code were numbered and rightly so, following the law laid down in Puttaswamy, the Section 497 of the IPC was held to be Unconstitutional.The following excerpt from the judgement will be determinative of the path that will be charted by the Indian Data Protection regime for years to come

> "*Liberty has a broader meaning of which privacy is a subset. All libertiesmaynotbeexercisedinprivacy.Yetotherscanbefulfilledonlywithin*

seriouslywhileatthesametimeprotectingtheprivacyentitlementsofwomengroundedinthe identity of gender and liberty.

[415] *Id.*at39.

aprivatespace.Privacyenablestheindividualtoretaintheautonomyofthe body and mind. The autonomy of the individual is the ability to make decisionsonvitalmattersofconcerntolife.Privacyhasnotbeencouchedas an independent fundamental right. But that does not detract from the constitutional protection afforded to it, once the true nature of privacy and its relationship with those fundamental rights which are expressly protected is understood. Privacy lies across the spectrum of protected freedoms. The guaranteeofequalityisaguaranteeagainstarbitrarystateaction.Itprevents the state from discriminating between individuals. The destruction by the state of a sanctified personal space whether of the body or of the mind is violativeoftheguaranteeagainstarbitrarystateaction.Privacyofthebody entitles an individual to the integrity of the physical aspects of personhood. The intersection between one's mental integrity and privacy entitles the individualtofreedomofthought,thefreedomtobelieveinwhatisright,and the freedom of self-determination[416]".

TheSection497ofthe IndianPenalCode thatcriminalizedadulterywasbasedupon the notion of romantic paternalisation of women and sought to treat women as a chattel,ownedbytheirhusbands.Holdingthatthedecisionalprivacywasaninherent aspect of the right to dignity, the Supreme Courtmarked the herald of the chapter of decisional privacy in the Indian scheme.

In*NavtejSinghJauharv.UnionofIndia*[417],theSupremeCourtonceagainfollowing its ration in KS Puttaswamy decriminalized the hitherto offence of "homosexuality" on the grounds of unwarranted inference in the right to decisional privacy of the individuals.Thecourtheldthatthescopeoftherighttoprivacyisquitebroad under the Indian constitutional scheme and it encompasses within its fold the decisional, spatialandinformationalprivacyaswell.Therighttoprivacyisinherentlyrelatedto the to the autonomy in making personal choices related to food, sexual choices, religionetc.andtheunwarrantedinterferenceofthestatewouldtantamountto

[416]2018SCCOnLineSC 1676

[417](2017)9SCC1

violation ofthefundamental right to privacy oftheindividuals. TheCourt thenwent on to observe that:

> *"Privacy enables each individual to take crucial decisions which find expression in thehuman personality.Itenables individuals to preservetheir beliefs, thoughts, expressions, ideas, ideologies, preferences and choices againstsocietaldemandsofhomogeneity.Privacyisanintrinsicrecognition of heterogeneity, of the right of the individual to be different and to stand againstthetideofconformityincreatingazoneofsolitude.Privacyprotects the individual from the searching glare of publicity in matters which are personal to his or her life*[418]*."*

Thesubsequentdecriminalisationoftheoldnotionsoftherighttoprivacywhichwere invariably attached to the social relations have established the fact that the Supreme CourtofIndiahaslaidthefoundationsofarobustprivacyprotectionregimeinIndia. However, does that foundation help in establishing a healthy data protection regime in India will depend a lot on the course adopted by the legislature.

Theanalysisinthepresentchapterdealtwiththefacetsoftheexistingdataprotection regime in India. A bare perusal of the existing legislations and the precedents showcaseaverypoorpictureofthedataprotectionregimeinthecountry.Ithastobe ceded that the Indian society as whole including the constituent assembly was not open to the idea of accepting the right to privacy as a distinct right that could be attached to dignity and the right to life and liberty.Following the same line of thinking,theConstitutionalCourtsinIndiatookoversevendecadestorecognizethe existenceofadistinctrighttoprivacy withintheIndianConstitutionscheme.Asfar as data protection is concerned, the initial approach of the Indian legislature was to tacklethegrowinginstancesofthedatatheftandfraudintheboomingIndian

[418]NavtejSinghJauharv.UnionofIndia,(2017)9SCC1

Information Technology sector. Thefact that the driving forcebehind the enactment of the Information Technology Act, 2000 was the objective to curb the growing menace of cyber fraud and not the issue of data protection resulted into a very weak data protection law in India.

In the absence of a comprehensive data protection law in India, one has to look for the provisions in various other legislations that are aimed at the providing adequate security to the personal data of the individuals. Some of the enactments that do seek to protect the informational privacy of the individuals do include the Information Technology Act, 2000 and the Information Technology Rules 2011, and the finder has analyzed the various provisions of these enactments to gauge the effectiveness of the existing data protection regime in India.

a) IndianDataProtectionadoptsaveryfeebleapproachtowardsdataprotection andisill-equippedwithprovisionsthatcan'taffordprotectiontothepersonal data of the individuals.

b) ThegloballyacceptedDataProtectionPrincipleshavenotbeenadoptedunder the Indian Data Protection regime in India.

c) With the State being the largest processor of data, the law should afford sufficient safeguards against the possibility of invasion to the right to data privacy by the state. The current data protection framework in India is inapplicable to the State-actors which renders it impossible to protect the unwarranted data breach by government and its agencies.

d) Thelackofadequatemechanismstoguaranteeandenforcethedataprotection principlesareabsentinthelawsatpresentandthereisadireneedtopropela paradigm shift in the approach of the legislature to confer the ownership of data to the data principals.

e) There is a need to have an independent Data protection Authority in India to enforce the rights of individuals against data breaches. Currently there is no

provision mandating the establishment of a data protection authority and the whole adjudication framework of data breach claims are manned by the executive.

f) Theprovisionsoftheexistingdataprotectionregimeinindiahavenegligible emphasis on the data security measures and hence there is a need to include theprovisionsregulatingthesocialmediaintermediariesanddatalocalisation.

g) TheInformationTechnologyAct,2000posesagreatdealofbarriersuponthe enforcementoftherighttobecompensatedonthegroundsofdatabreachand thus makes it unfriendly to the rights of data principals.

h) The existing data protection framework lacks the key principles of data protection such as the right to erasure, the right to informational self-determination, right to informed consent, the right to be forgotten etc.

i) The existing regime doesn't offer any protection to the children's data and fails to include them within the meaning of personal data.

j) The obligations of the data processors are extremely curtailed in their ambit andthusitbecomesextremelydifficulttosecuretheremediesthathavebeen provided for in the existing laws.

k) The entire framework lacks to incorporate the provisions to tackle the threat of breach of data by using the new technological advancements. The provisions relating to anonymization and privacy by design are completely absent.

l) TheSupremeCourtofIndiahasuppedtheanteagainsttheexistinglacunasin the Data Protection regime in the country and by holding that the right to informational self-determination was an inherent aspect of the fundamental

righttoprivacy,theapexcourthaslaiddownthefoundationsofarobustdata protection framework in the country.

Overonethirdofadecadehas already passedsincetheday theRighttoPrivacywas recognizedasafundamentalrightguaranteedbytheConstitutionofIndia.However, wehaveseenaverylittleprogressinthedirectionofenactingacomprehensiveData Protection Lawin India and theproposed DataProtection Bill, 2019 is yet to seethe light of the day. Since the finder has extensively considered the legislations concerning the Data Protection regime in India

CHAPTER 5: COMPARATIVE STUDY OF THE DATA PROTECTION REGIME IN INDIA WITH REFERNCE TO EU,US &UK

5.1 Introduction

The Previous Chapter has dwelled into the intricacies of the existing data protection regime in India and has enabled the finder to formulate a rational opinion with regards to the existing state of affairs in the realm of data protection in India. With a majorportionofgroundworkbeingaccomplished,thefindershallinthischapter proceed to contrast some of the Key aspects of the existing and the proposed data protection law in India. Thesole object of this discussion is to churn out the feasible andpracticalsuggestionsinordertoaccomplishtheobjectiveofestablishingarobust data protection framework in India.

ThefindershallexaminetheprovisionsoftheInformationtechnologyAct,2000, The SDPI Rules, 2011 and the Personal Data Protection Bill, 2019 to test the dissertation, "*The Legal framework for Data Protection in India is not adequate to protecttherighttoPrivacyofthecitizens*."Wehavealreadytakenintoconsideration, theapproachthatthejudiciary,inIndia,hastakenwithregardstovariouscontoursof right to privacy and thus the discussions in the upcoming sections shall be limited purelytotheanalysisoftheprovisionsoftheexistingandtheproposeddataprotection lawsinbillandtheirimplicationswithregardstotheupcomingdataprotectionregime in India. The detailed analysis of the key provisions of the proposed bill be instrumental in determining the outcome of the dissertation.

TheprimaryfocusoftheresearchwillbetocomparethedataprotectionlawsofIndia to those of European Union, the United States and the United Kingdom and some of the BRICS countries. Given the fact that as of know there exists peace-meal legislation in India that regulates the Data Protection, in order to establish a synergy betweenthe researchworkandthepracticalities,thefinderhaschosentocompare

the provisions of the proposed Data Protection Laws in India in its entirety. There's no prize forguessing that thedays of theexisting dataprotection regimein Indiaare numberedandinamatteroflessthanayear,wemayhaveanallnewdataprotection regime in the place and hence it becomes imperative to keep a tap on the changing dynamics of the data protection legislation in the country. Keeping this normative aspect in view, the finder shall compare some of the most vital aspects of data protection laws in India with those of European Union, the United States and the United Kingdom.

5.2 Scope of The Indian Data Protection Laws in India and Elsewhere

The preamble of GDPR is extremely broad and lays down through over 168 recitals the object behind enactment of the regulation[419]. The recitals set out in the broadest oftermstheneedofenactingtheprovisionswhilerecognizinginmostcleartermsthe fundamental right to privacy. Similarly, the preamble of the UK Data Protection Act goesas,"*AnActtomakeprovisionfortheregulationoftheprocessingofinformation relating to individuals; to make provision in connection with the Information Commissioner'sfunctionsundercertainregulationsrelatingtoinformation;tomake provision for a direct marketing code of practice; and for connected purposes*." It is submittedthatthepreambleofanylegislationisn'tamerecustomaryformalityandit essentiallysetsthetoneandtenorofthelegislation.Itisalsooneofthemajorsources of judicial interpretation of the provisions of the any law. Hence, it is necessary that the preamble entails within its definition a broad set of ancillary objectives without gettingdeviatedfromthepithandsubstanceofthelegislation.However,thepreamble oftheITAct2000doesn'trefertotherighttoprivacyevenonce.Given thefactthat India lacks a comprehensive data protection legislation to this date, a comparison between GDPR and the ITAct and the IT rules will do no justiceto the comparison, keepingthisnormativeaspectoftheanalysisinmind,thefinder,forthesakeof

[419]See,PreambletoUKDataProtectionAct,2018.

qualityofanalysisshalltakeintoaccountthevariousprovisionsoftheproposedData Protection Bill in the fold of Indian data protection regime. The Personal Data Protection Bill, 2019 as it has been named, is aimed at providing a robust data protection regime in the country that would accord the right to data privacy of the citizens[420] and thus it becomes absolutely necessary for the preamble of the law to specify in unequivocal terms the objectives for which it is being brought.It also providesthatthatitisaconstitutionalnecessitytoprovideprotectiontopersonaldata is "*an essential facet of informational privacy*."

It ought to be highlighted that the preamble of the proposed Indian Act, unlike the GDPRpushesforthepromotionofdigitaleconomyandpitchesfordigitalgovernance instead of laying emphasis on the importance of informational privacy. It also recognizes that in the era of digital economy, data has become an essential means of communication and hence they deserve a greater degree of protection, but undue emphasisontheaspectoffosteringdigitaleconomywhilepushingthefocalaspectof furtheringthegoalofsecuringtherighttoprivacyisanalarmingaspect.ThePersonal Data Protection Bill 2019, which is supposedly the bedrock of the upcoming data protection regime in India doesn't explicitly recognize the aspect of informational self-determinationinasmuchasrighttoinformationalprivacyisconcernedandthus raises serious apprehensions about the effectiveness of the proposed data protection regime in India[421].

Amongotherthings,thebillalsoproposestolaydownadetailedframeworktocreate adataprotectionregimethatpromisestoimplementtechnicalandstructuralmeasures to regulate processing of personal data, prevention of unauthorized used of personal databutdoesn'trecognizethedataprincipalastheowneroftheirdata.Theproposed billalsoseekstoestablishadataprotectionauthoritytosecuretheseobjectivesbut

[420]ThePersonalDataProtectionBill,2019,pmbl,No.373,BillsofParliament,(India2019).

[421]AparGupta,NotesfromaDigitalRepublic,InternetFreedomFoundation(January26,2020), https://internetfreedom.in/our-digital-republic/.

fails to highlighted the aspect of autonomy attached to the authority[422]. The fact that thedataprotectionregimeinIndiaisatanascentstageandlackofjudicialprecedents (barring Puttaswamy) leaves us with no option other than relying upon the meaning, facets and limitations of right to privacy and thus the an ideal preamble of a data protectionlawinacountrylikeIndiashouldhavebeenliberalinitsapproachtowards highlighting the importance of protection of right to informational self-determination[423].Indiadoesn'thavetheadvantagepossessedbytheEuropeanUnion where the judiciary has already developed a great deal of jurisprudence on Data Protection. Even the various United States legislationsdo vouch for providing adequate degree of protection to the right to privacy of the citizens in the preambles on the other hand the preamble of the proposed bill, makes no mention of the noble objective of placing the rights of the data principals over any other aspect of data processing. A similar inference can be drawn from the analysis of the various other data protection legislations in the United States such as the Health Insurance Portability and Accountability Act, 1996 and the Fair Credit Reporting Act.

While, committing to foster a digital economy and promoting innovation, the proposed bill puts protection of rights of the individuals to the back seat[424]. It is submitted that the failure of the preamble of the bill to expressly incorporate the objectiveofprotectionofrightsofdatasubjectsagainstinvasionbystate,asinahuge majority of the cases, the data controller is the state itself may be detrimental to the causeofputtingarobustdataprotectionregimeinplace.Thebillshouldalsoprovide incleartermsthemethodsinwhichtheobjectiveoffurtheringdataprotectionregime issoughttobeachieved.UnliketheGDPR,thebillinitspresentform,givesthe

[422]SohiniBagchi,DataPrivacyDay:India'sPDPBillNeedsClarification,(Jan. 28, 2020, 8:14 am), https://www.cxotoday.com/news-analysis/data-privacy-day-indias-pdp- bill-needs-clarification/.

[423] Swathi Moorthy, Data Protection Authority Will Be A Government Stooge And Weaken Personal Data Bill: Justice BN Srikrishna, (January 30, 2020, 12:18 IST), https://www.firstpost.com/tech/news-analysis/data-protection-authority-will-be-a-government-stooge-and-weaken-personal-data-bill-justice-bn-srikrishna-7976651.html.

[424]*Id.*At47.

economicaspectofthedataprecedenceovertherightsofthedataprincipals.Thefact that the preamble ignores the need for establishing a transparent surveillance regime which would be subservient to the rule of law and undue emphasis on fostering a digital economy and "*ensuring empowerment, progress and innovation through digital governance*[425]" while omitting the need for good governance, does indicate a genesis of data protection regime that treats the data of the citizens more as a tool of commercialization.

It is submitted that the bill should incorporate, within its realm the principle that the data principal is the true owner of their data and right to informational self-determination and decisional autonomy is the key aspect of the proposed data protection regime. While fostering digital economy and digital governance may be focal to the policy of the government, these objectives shouldn't be allowed to push the greater cause of protecting the right to privacy to the back seat. The preamble ought to include in unequivocal terms, the guarantee of protection against the interference of the state in the private domain of the individuals and pitch for surveillance reform in India. Contrasting the preamble of the bill with that of GDPR shows the inherent lacunas that have found their foot in the very inception of materialization of a robust data protection regime in India[426].

5.3 Application of Act to Processing of Personal Data.

TheInformationtechnologyAct,20000 and theSDPIRules,2011do notrenderany protection whatsoever to the personal data of the individuals unless that data falls within the definition of sensitive data.Notably some aspects of the informational privacy are covered by the Telegraph Act. The Telegraph Actand Rules, which contains provisions that prohibit and penalize unlawful interception of communication.Furthermore,licensesissuedtotelecomserviceproviders(TSPs)

[425] *Id*.At47.

[426] RyanM.Calo,*AgainstNoticeSkepticisminPrivacy(andElsewhere),*87(3)NOTREDAMELAW REVIEW, 1031 , 1033-37(2012).

under thisActrequire TSPs to take measures to safeguard the privacyof their customersandconfidentialityofcommunications.[427]Moreover,theprovisionsofthe Act do not apply to the public entities. It is submitted that such exclusions do make the promise of data protection hollow and namesake. However, in the sharp contrast to it, the GDPR offers complete protection to the personal data of the individuals while recognizing the right to have protection of personal data as a fundamental right[428]. The application of the Act is both territorial and extra territorial and applies to the entities based outside India as well, if the processing of personal data by them concerns with any business or any specific activity in India. In as much as the application of the act is concerned, the scope of GDPR, US dataprotection laws and the UK Data Protection Act are similar[429]. The provisions of the Act shall be applicable in the following cases[430],

- Thedataisbeingprocessed,collected,storedordisclosedwithintheterritoriallimits of India.
- The data is processed by the State, any company based in India or any other juristic person of India.
- TheprocessingofdataconcernsprofilingofdatawithintheIndian territory.
- The processing of data by the fiduciaries or data processors not present within the territory of India, if such processing is in relation to business committed in India or any other specific activity.

Whiletheproposedbilldoesdoawaywithmajorshortcomingofpreviousapplication of the provisions to the non-sensitive personal data, there are some of the loopholes thatmakeeventheupcomingdataprotectionregimeweakerthantheGDPRinterms ofprotectionaccordedtotherighttoprivacy.Oneofthe mostpeculiaraspectsofthe

[427]PrivacyandTelecommunications:DoWeHavetheSafeguards? —TheCentrefor Internet and Society, Cis-india.org (2021), https://cis-india.org/internet-governance/blog/privacy/privacy-telecommunications

[428]Article1(1)GDPR

[429]SeeArticle3GDPR

[430]ThePersonalDataProtectionBill,§2,*supra*note 47.

proposedbillistheexclusionof"non-personal"datafromtheambitoftheActwhich givestheCentralgovernmentanimpunitytodenyprotectionsprovidedundertheAct to such data. It is submitted that the definition of the term non-personal data is quite vague and illusionary at the same time. It is submitted that a piece of legislation that isbeingbroughtwiththeobjectiveofprotectingthepersonaldataofthecitizensand creatingahealthydataprotectionregime,shouldn'tincludewindowsforenablingthe breach of informational privacy by including the clauses like "non-personal" data[431] and exempting them from the application of the proposed Act. With extensive development in technology and advancement of artificial intelligence, even the data that doesn't have characteristic of individual identifiable information can be transformed into personal data[432]. It is submitted that the possibilityof misuse of the non-personal data shouldn't be ignored altogether. On the other hand, the GDPR, THE UK Data Protection Act and the US Privacy legislations don't provide for any such classification.

5.3.1 Personal Data, Non-Personal Data and Sensitive Data

One of the first loopholes in the proposed bill emerges in the form of a blanket ban ontheapplicationoftheprovisionsonnon-personalwhileblindlyadoptingthetrends in global jurisdictions[433]. Before, commenting upon the aspects related to these definitions that may be detrimental to the prospects of an effective data protection regime in India, it would be optimal to discuss in a nutshell the definitions of these terms as proposed under the bill.

[431] ThePersonalDataProtectionBill,§91,*supra*note47.

[432] IanWalden,AnonymizingPersonalData,10INT'LJ.L.&INFO.TECH.224,229-233(2002)

[433] JflrgenSchaafandThomasMeyer,OutsourcingtoIndia:CrouchingTigerSettoPounce,Deutsche Bank Research (Oct. 25, 2005), http://www.dbresearch.com/PROD/DBRINTERNETENPROD/PROD0000000000192125.pdf.

5.3.1.1 PersonalData

Thedefinition ofpersonal datain theGDPRand theproposed bill arealmost similar but what makes the Indian approach weaker is the inclusion of the concept of non-personal data. As per, the proposed Bill, provides comprehensive definition of the term personal data and expressly differentiates between personal data, non-personal data and sensitive data. The report relied extensively on the observations in Puttaswamyandreiteratedthatthe,"*sphereofprivacyincludesarighttoprotectone's identity*" and the definition of the personal data in the proposed bill is based on the same line of reasoning.As per the proposed bill:

> *"Personaldata"meansdataaboutorrelatingtoanaturalpersonwho is directly or indirectly identifiable, having regard to any characteristic,trait,attributeoranyotherfeatureoftheidentityofsuch natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling*[434]."

Itmaybenotedthattheterm"personaldata"hasbeengivenaverywideandmeaning andreferstoallthepersonallyidentifiableinformationthatcanbeusedeitherdirectly or indirectly to identify a natural person. It also covers within its scope all the data which when combined can be used to relate to any trait or characteristic of a natural person. The proposed bill does endorse the recommendation of BN Srikrishna Committeereportthathadsuggestedthata"flexibledefinition"ofpersonaldatamust be laid down in the legislation. The report also clarified that the flexible definition must not come at the cost of certainty and at the same time it must be conducive to theincorporationofnewtechnologicaldevelopmentsthatmayalterthecategoriesof data.[435]

[434]ThePersonalDataProtectionBill,§2(28),*supra*note47.

[435] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, (Jan. 20, 2020, 3:40 pm), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

> *"definition of personal data centered on identifiability must be constructed with the full awareness that its scope will, in many cases, depend on the context, in which the relevant data is being processed. Bearing this mind, we believe that a broad and flexible definition of personal data should be adopted"*

The proposed bill does incorporate all the recommendations regarding the width of the definition of personal data and, it must be acknowledged that the legislature, as far as the definition of personal data is concerned, the recommendations of the committee have been extensively incorporated. It is submitted that as far as the definitionofpersonaldataisconcerned,theproposedIndianlawandtheGDPRhave adopted a similar approach. The judicial precedents of the United States too seem to be following the same path.

5.3.1.2 SensitiveData

TheITAct,2000andtheSDPIRules,2011doconferprotectiononlytothepersonal data that is sensitive in its character. While recognizing the element of dignity attachedtotherighttoprivacyundertheconstitutionalscheme,theSCinPuttaswamy has ensured greater protection to the data have direct bearing on the core traits of individuals.TheBNSrikrishnaCommitteereport,highlightedthepointthat,"*certain categoriesofpersonaldatamaybelikelytocausegreaterharm,orharmofagraver nature*[436]" while endorsing the need for separate delineation of such data.As per, RamaVedashree,"*conceptofSensitivePersonalDataisprimarilyusedforproviding higherlevelprotectiontothedatasubjectfrominstancesofprofiling,discrimination andinflictionofharmthatareidentitydriven*[437]."Theproposedbilldefinessensitive informationtoinclude,biometricdata,geneticdata,healthrelatedinformation,

[436] Aroon Deep, *The dissenting voices in the Srikrishna Committee's Data Protection report*, MEDIANAMA (July 28, 2018),https://www.medianama.com/2018/07/223-srikrishna-dissent/.
[437] *Id.*

information related to caste, religious belief, sex, sexual orientation, political affiliation, caste, intersex status or any other officially identifiable information.

5.3.1.3 FinancialData

Theexistingprovisionsconcerningtherighttodataprotectioninindia,docategorize the financial data as a sensitive data and thus provide them protection from unwarrantedinterferences.ThepersonaldataprotectionBill,2019alsorecognizesthe financial data as sensitive data. As per, the Bill, *"financial data" means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal includingfinancialstatusandcredithistory*[438]*."*ThiswouldmeanthatthePAN, Income tax details, bank details, insurance details and related information will be consideredassensitivedataandthustherewillbegreaterlevelofprotectionaccorded to them.

Fair Credit Reporting Act (FCRA)[439], in the United States too grants a great degree of protection to the financial data of the citizens and mandates the credit rating agencies to guarantee confidentiality of the financial data of the customers. The Act also mandates that the credit agencies have to provide notification to the customers about the data that can be used against them. "*This obligation the part of the lenders tonotifytheconsumersabouttheinformationthatisusedagainstthemgivestheman opportunitytoknowandif possible,challengetheinformation.TheActalsoimposes a duty upon the rating agencies to inform the consumers about the details of the information.OneoftheotherwaysinwhichtheFCRAseekstoguaranteetheprivacy of the consumers is by assuring the confidentiality of the data*[440]".

[438]ThePersonalDataProtectionBill,§2(18),*supra*note47.
[439]15U.S.C.§1681
[440]SupraNote

5.3.1.4 HealthData

TheHealthInsurancePortabilityandAccountabilityAct(HIPAA)doesaffordagreat degree of protection to the personal health data of the individuals and bars their processing without consent. The fact that the medical history includes sensitive information about the medical and health background of the individuals makes their protection an indispensable aspect of right to privacy. The provisions of HIPAA ensure that the sensitive information related to the right to privacy are guaranteed ampleprotection.Ontheotherhand, as wehaveobservedin theprovisionsofthe IT Act 2000 and the SDPI Rules, 2011 and the various rules of the medical council of India, there exists a contradiction amongst the provisions about the legality of the processing of health data. Even though the SDPI Rules, 2011 do categorize the data related to the medical history as sensitive data, the non-application of the provisions to the government agencies leaves a major window for privacy breach.

In the European Union as well, as we have observed in the previous chapters, the catena of judgments of the ECtHR have highlighted the importance of providing adequate protection to the data concerning medical history of the individuals[441]. The draft bill takes a cautious approach while including all details related to the medical history of an individual and does include a very exhaustive definition of the health data. As per of the proposed bill, "*health data means the data related to the state of physical or mental health of the data principal and includes records regarding the past,presentorfuturestateofthehealthofsuchdataprincipal,datacollectedinthe course of registration for, or provision of health services, data associating the data principal to the provision of specific health services."*[442]

Itmaybepointedoutthattheprovisioncompletelyendorsedthefactthattheeventhe minutestdetailsrelatingtothemedicalhistoryofanindividualmaybedetrimentalto thedignityoftheindividualandhencemustbeconferredgreaterprotection.Atthis

[441]K.H.andOthersv.Slovakia,ECtHR,K.H.andOthersv.Slovakia,No.32881/04,28April2009
[442]ThePersonalDataProtectionBill,§2(21),*supra*note47.

juncture, the judgment in Mr. X v Hospital Z[443], where the SC had observed that the provision has been acknowledged in letter and spirit where in the SC had noted that,

> "*Privatefactsmayamounttoaninvasionoftheright ofPrivacywhich maysometimesleadtotheclashofoneperson's"righttobeletalone" with another person's right to be informed. Disclosure of even true private facts has the tenancy to disturb a person's tranquility. It may generate many complexes in him and may even lead to psychological problems[444].*

Theproposedbillplacesthehealth-relateddatatounderthecategoryofsensitivedata andthusaccordsagreaterlevelofprotectiontoit[445].Thebilldoesstrivetofulfillthe existingvoidintheprotectionofsensitivenatureofmedicaldatawhicharecurrently governedbytheIMCcodeswhicharen'tadequatetoconferprotectionandsafeguards mechanism to sensitive medical data. Also, the present data protection regime absolutely offers no protection to the personal data in the public sector medical institutions,howeverasperthePreambleoftheproposedbill,thisvoidwillnolonger be in place and thus these safeguards will be applied to the public sector as well.

5.4 Data Anonymisation

The existing data protection regime in India offers a very negligible guide upon the existence of policy of anonymised data. Neither the Information Technology Act, 2000 nor the SDPI Rules 2011 have any provisions mandating data anonymisation. On the other hand, the global jurisprudence on the principles of data anonymisation is abundant and extremely well developed. But theGDPR as well prescribes that the anonymised data that cannot be brought back to its original form, should not be exemptfromtheapplicationoftheprovisionsoftheregulation.Theproposedbill

[443]Mr.Xv.HospitalZ, AIR1999**SC**495.
[444]*Id.*
[445]ThePersonalDataProtectionBill,§3(21),*supra*note47.

does incorporate the principle of data anonymisation to change the characteristic of the personal data. As per, the recommendations of the B N Sri Krishna committee whichhadsuggestedadherencetotheprincipleofdataanonymisationinordertocurb themisuseofpersonallyidentifiableinformation.TheActprovidesabroaddefinition of data anonymisation and provides that:

> *"anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority*[446]*;*

While, the principle of data *anonymisation,* isn't peculiar to the data protection regimes all over the world, the tangled web of treachery by the state to process the personaldatacertainlyis.Theproposedbillatthefirstinstanceignoresthepossibility of the de-anonymisation of the anonymised personal data through the technological developmentsinthefutureandproceedswiththisunscientificpresumptiontocompel any processor to share these anonymised personal data for the better targeting of the service[447].

To put this in simpler terms, the central government can compel the data fiduciaries to share the anonymised and non-personal data of the citizens for the purposes of evidence-based policy making and bettertargeting ofservice. It is submitted that the proposed bill lacks a comprehensive definition of anonymised data and the non-personal data. The bill also ignores the possibility of process through which the anonymised and non-personal data could be turned into personally identifiable data. Equally worrying is the fact that the central government can compel the data fiduciariestosharethedatainthesecategoriesforevidence-basedpolicymakingand bettertargetedofservice[448].ThedissentingopinionofJusticeChandrachudinthe

[446]ThePersonalDataProtectionBill,§3(2),*supra*note47.
[447]ThePersonalDataProtectionBill,§91(1),*supra*note47.
[448]ThePersonalDataProtectionBill,§91(1),*supra*note47.

Aadhaar judgment had also expressed doubts over the irreversibility of the anonymised data.

5.4.1 Points of Concern

The most pressing concern regarding the non-personal data in general and the anonymised data in specific is the possibility of their conversion into personally identifiableinformation[449].While,theopinionofthecommentatorsallovertheworld has always been sceptical about the irreversibility of the anonymised data[450], the bill while leaving these concerns unaddressed, brings in another window for injecting uncertainty into the data protection regime in the form of non-personal data. At the veryoutset, thefinderwould liketo point outthat theinclusion ofterminologies like non-personal data was absolutely unnecessary and unworthy of a place in a data protection regime. As it will be noted in the subsequent chapters, it is highly likely that the Central government may harness the loophole to breach the informational privacy of the individuals[451].

The most formidable concern emerging out of the so-called anonymised data stems fromthepossibilityofitsreversibility.Itmaybenotedattheoutsetthatthedefinition of the anonymized data as adopted in the Bill is fallacious. The provision ought to expresslymentionthatforadatatobecategorizedasananonymiseddata,"*itcanbe no longer be used to identify a natural person by using "all the means likely reasonably to be used.*[452]*"* Instead of coming up with an objective and wholesome standard for determining the nature of data, the provisions leaves it upon the Data ProtectionAuthoritytoprescribethestandardsfordeterminingthestandardsof

[449] Paul Ohm, Broken Promises of Privacy: *Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1744-1769. (2010).

[450] *Id.*

[451] *Id.*

[452] CommonServs.Agencyv.ScottishInfo.Comm'r[2008]UKHL47.

irreversibility[453].Moreover, theprocessof anonymisationisn'triskfree. Itshouldbe noted that a data which is of the non-personal nature in the currents scenario, may obtain the character of personal data over a period of time[454].

It may be thus observed that the legislature has left open a wide window through whichthepersonallyidentifiableinformationunderthedisguiseofnon-personaland anonymized data may escape the application of the data protection law and thus jeopardize the fundamental rights of the individuals. One of the other worrying aspects ofthebill is thepowerofthecentral government to classifydataas sensitive data, which will be taken up later in discussion. However, the indifference of the legislature towards the risks posed by a cut and dried demarcation between the personal data and the anonymised data raises serious apprehensions about the effectiveness of the proposed data protection regime.

Unfortunately,thePersonalDataprotectionBill,2019,initscurrentform,ignoresthe argumentsagainstuniquenessofthebiometricdata,putforthbyJusticeChandrachud and bases, the definition of biometric data on its ability to, "allow or confirm the unique identification of the individual." The definition within the proposed bill provides that:

> *"Biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person;[455]"*

[453]SophieStalla-Bourdillon & Alison Knight, *AnonymousData v. PersonalData - FalseDebate: An EU Perspective on Anonymization, PseudonymizationandPersonal Data*,34 WIS. INT'LL.J. 284, 285-287 (2016).

[454]*Id.*

[455]ThePersonalDataProtectionBill,§3(7),*supra*note47.

The definition of biometric data under the proposed bill is based on the premise that the biometric data includes only those data which allow the confirmation of the personal identification of natural persons. By doing this, the proposed bill virtually paves the gateway for excluding a large volume of personal data on the pretext of their inability to provide enough information about the identity of an individual. Nonetheless,aspertherecommendationsofthecommitteethebillincludesbiometric data within the meaning of sensitive data and hence pitch for a greater degree of protection for such data.

5.5 Rights of Data Principles

No data protection regime that restricts the rights of the data principals can be instrumental in shaping a robust data protection regime. The very concept of informational privacy is anchored around the theme of informational self-determinationandadataprotectionlawmustnotonlyrecognizetherightsofthedata principals in the broadest sense; it should also provide adequate mechanisms to enforce these rights[456]. We have considered the scope of the rights of the Data PrincipalsinthejurisdictionsoftheEuropeanUnion,theUnitedStatesandtheUnited Kingdom.Thissectionisinvariablyaimedatcomparingtherightsconferreduponthe dataownersallovertheworldandtheIndiandataprotectionregime.Inordertowiden the scope of our analysis the finder will also consider some of the BRICS countries'dataprotection legislations. ThePersonal Data Protection Bill, recognizes the following rights of the data principals namely: Right to be forgotten[457], the right to correction and erasure[458], the right to confirmation and access[459] and the right to data portability[460]. It may be pointed out that the scope and extent of the rights recognized by the proposed law are quite limited.

[456]PeterBlume,PracticalDataProtection,2Int'lJ.L.&Info.Tech.194(1994);RupertBattcock,Data Protection: Where Next, 3 Int'l J.L. & Info. Tech. 156 (1995); Anneliese Roos, Core Principles of Data Protection Law, 39 Comp. & Int'l L.J. S. Afr. 102 (2006).

[457]ThePersonalDataProtectionBill,§20,*supra*note47.

[458]ThePersonalDataProtectionBill,§18,*supra*note47.

[459]ThePersonalDataProtectionBill,§17,*supra*note47.

[460]ThePersonalDataProtectionBill,§19,*supra*note47.

5.5.1 Principles for Protection of Individual's Data

As of today, the Information Technology Act, 2000 and the InformationTechnology(Reasonable security practices and procedures and sensitive personal data or information)Rules,2011 do provide a very a very restricted notion of the rights afforded to the data principal. The provisions of the bill, do adopt an abridged versionoftherightsofthedataprincipals,whichmightbedetrimentaltotheobjective ofarobust dataprotection regimein India.Thus, it becomesoptimal to haveaadopt a liberal approach in recognizing the rights of the data principals. The rights guaranteed under the proposed bill concerning the right to correction, completion, updationanderasureofdatahavesubstantiallybeencurtailedundertheprovisionsof the bill. This right of the data principal has been made conditional upon the obligations of the data fiduciary. The provision places forth a complex web of procedure for enforcement of the right, which is unbecoming of a robust data protection regime.

WhatreaffirmsthepropositionofthefinderthatthePersonalDataProtectionBill 2019, is actually a data grab bill is the sheer indifference of the legislature towards the rights of the data principal. The bill recognizes a fairly low number of rights of thedataprincipalandthusleavesawideroomforabuseoftherighttoprivacybythe datafiduciaries.However,itmustbenotedthatthattheapplicationoftheserightsare quite limited in their scope and thus there is a need to adopt an exhaustive sets of rightsofthedataprincipalsunderthebill.Thefollowingrightsofthedataprincipals couldbeincorporatedforcreatingadataprotectionregimethatis"protective"ofthe rights of the data principals in the truest sense[461]. The bill recognizes The right to informedconsent, Therighttodatasecurity,TherighttoInformationalPrivacy,The right to know, Right to object, Right to free withdrawal of consent, Right to informational self-determination.

[461]SreenidhiSrinivasanandNamrataMukherjee,*Buildinganeffectivedataprotectionregime*,VIDHI CENTRE FOR LEGAL POLICY, New Delhi (2017).

Interestingly, one may find some of these rights in the form of obligation for data fiduciarywithinthebill,however,itissubmittedthattheinclusionofthesepriciples withintherightsofthedataprincipalwillaccordthemagreaterprotectionagainstthe threats to the right to privacy[462].It is submitted that, in order to have a robust data protection regime in India, the bill must not shy away from granting the data principals adequate rights so as to empower them to take recourse to the law in case of even a minimal breach of data privacy[463]. While, it is appreciable that the bill includes the concepts such as privacy by design and notifications about the breach under the obligations of data fiduciaries, the failure on the part of the legislature to adopt same principles within the framework of rights of the data principal doesn't serve the cause of a healthy data protection regime[464]. Hence, the legislature should make it a point to include these exhaustive rights within the rights of the data principals so as to accord a greater degree of protection to the rights of the data principals. This would also rightfully tilt the balance of convenience in favor of the data principals as against the existing position.

ContrastitwiththerightsconferreduponthedataprincipalsintheGDPR.TheGDPR doesn't mince its words and provides a very wide meaning to the rights of the data principals. It provides as many as 12 rights to the data principals including the right to erasure and the right to data portability, these rights are notably omitted in the proposed Indian data protection regime.

The Indian awakening about the right to privacy has been rather delayed by over at least three decades[465]. One of the most notable objectives behind introduction of the personaldataprotectionbill,2019istopromoteconsciousnessamongsttheIndians

[462]NandanNilekani,DatatothePeople:India'sInclusiveInternet,97FOREIGNAFF.19(2018).
[463]*Id.*
[464]UmangJoshi,OnlinePrivacyandDataProtectioninIndia:ALegalPerspective,7NUALSL.J.95 (2013).
[465]*Id.*

about the importance of right to privacy and affording adequate security to the personaldata.However,theproposedbilldoesn'tseemtodoenoughtomeetitsnoble objectives.WhatIndianeedstodayisarobustdataprotectionregimethatisextremely sensitive to the rights of the data principal, a law that would not only protect the citizensfrompossibledatabreachesbutalsoempowerthemdetectandseekremedies against the breach of right to privacy.The bill proposes to adopt an approach that would virtually make it impossible for a majority of the Indians who live below povertylinetospendmoneyforgettingtheirrightsunderthepropos edActenforced. The proposed bill categorically states that the it is open for the government to allow thedatafiduciariestoimposefeesonthedataprincipals,ifatalltheywishtogettheir recognized rights under the bill to be enforced[466].It is submitted that the legislature hasnottakenintotheaccount,theindifferenceofIndianpopulationtowardstheright to privacy and posed another barrier in the pursuit of getting their rights under the upcoming regime to be enforced. It is extremely difficult to comprehend that a Data Protection regime would expect, the data principals, who are least aware about their privacy right, will have to pay fees to their data fiduciaries to get their "own rights" enforced[467].Itissubmittedthatthelegislaturemustdoawaywiththeclauseof"fees" in order to show its commitment to informational self-determination.

TheGeneralDataProtectionLaw,GDPLalsoincludesawiderangeofprinciplesfor processing of personal data and stipulates that the data has to be processed in accordance with the principles of purpose limitation, transparency, fairness and lawfulness.[468]Notably,theGDPLalsoprovidesthatthedataprincipalwillbeentitled to seek any information about data free of cost, unlike the proposed personal Indian Data Protection law that seeks to dis-incentivize the data principals including the provision for imposition of fees by data processors for providing any information aboutthedata.TheGDPLismilesaheadofitssupposedIndiancounterpartwhenit

[466]ThePersonalDataProtectionBill,§21(2),*supra*note47.

[467] Stephen Mason, *Electronic Signatures in Law*, School of Advanced Study, University of London, 2016, pp. 387–396. *JSTOR*, www.jstor.org/stable/j.ctv5137w8.23. (Accessed 13 February 2020)

[468]Article46,GDPL (Brazil)

comes to affording respect to the notion of individual's control of their data. It providesthatthedatahastobeprocessedonlywiththeconsentofthedataprincipals barring very few instances. Moreover, the data processer is under an obligation to inform the data principal about the breaches of data in every case without any exceptionwhatsoever.ItmustbepointedoutthattheGDPLputsthedataprincipalin thedrivers'seatasfarastheprocessingofdataisconcernedandvestsunderthemthe authority to give and withdraw their consent for processing of data anytime[469]. It should be noted that this aspect of the Brazilian law is strictly in resonance with the principles of informational self-determination unlike the Personal Data Protection Bill.

TheGDPLprovidesthat therequirementoftheconsentofthedataprincipalwillnot be necessary for the processing of personal data only in a very limited number of cases. The Article 11 provides that[470]

> "*The processing of sensitive personal data shall only occur in the following situations: I – when the data subject or her/his legal representative specifically and distinctly consents, for the specific purposes;withoutconsentfromthedatasubject,inthesituationswhen it is indispensable for:*
> *a) controller'scompliancewithalegalorregulatory obligation;*
> *b) shared processing of data, when necessary, by the public administrationfor the execution of public policiesprovided in lawsor regulations;*
> *c) studiescarriedoutbyaresearchentity,wheneverpossibleensuring the anonymization of sensitive personal data;*

[469]Article13,GDPL (Brazil)
[470]Article11,GDPL (Brazil)

d) the regular exercise of rights, including in a contract and in a judicial, administrative and arbitration procedure, the last in accordance with the terms of Law No. 9,307, of September 23, 1996."

Onemaynoticethestrikingdifferencebetweenthestandardssetoutbytheir legislature while determining the cases wherein there can be a deviation from the principleofinformationalself-determination.TothecontraryoftheIndianapproach, theBrazilianlawprohibitstheprocessingofsensitivedatawithouttheconsentofthe data principal except in just 4 cases. These exceptions are quite justified for the functioningofastateandtheyareonthelinesofgroundsidentifiedundertheGDPR.

5.6 Obligations of Data Fiduciary

The proposed bill seeks to place obligations upon the data fiduciaries in as much as processing of personal data is concerned. As we have already discussed under the previous chapter, the global data protection regimes are based upon the data protection principles that are aimed at maximizing the scope of data protection. In a nutshell, this section shall analyze the principles that the present Personal data protectionbillproposestoadoptintheIndiandataprotectionlawregime.Attheonset, it must be acknowledged that the Bill takes all the eight data protection principles enshrinedundertheEuropeanlawsandseekstomouldthemintotheIndian scheme. Nonetheless,itwouldbefairtohaveabriefoverviewoftheseprinciplesastheyhave been adopted under the proposed bill.

5.6.1 The lawfulness, fairness and transparency of processing principle

The principal bars processing of personal data and only in cases where such processing is *necessary, specific and lawful*, such processing is allowed[471]. The section5oftheproposedbillseekstoincorporate thefairnessprincipleandprovides

[471]Evans,A.C."*EuropeanDataProtectionLaw*."29THEAMERICANJOURNALOF COMPARATIVE LAW, 570, 571-82 (1981).

that every person processing personal data must do so in just, fair and reasonable manner in order to ensure that the privacy of the data subject is not violated. What wouldqualifyasthe"just,fairandreasonablemannerisnotexplicitandwillhaveto be interpreted from the judicial precedents. As per the precedents, the test of arbitrariness would be applied by the courts to decide whether the data has been processed in a lawful and fair manner.

The genesis of the concept of "consent" can be traced in the Indian constitutional scheme in the Puttaswamy judgment itself. While emphasizing on the aspect of consent, Justice Nariman observed, "*informational privacy… does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may havecontrol over the dissemination of material that is personal to him.Unauthoriseduseofsuchinformationmay,thereforeleadtoinfringementofthis right*[472]*."*

5.6.1.1 ThePrincipleofPurpose Limitation

Theproposedbillprovidesthatwhenthedatasubjecthas consentedtoprocessingof data, such data shall not be used for any purpose other than the one for which the consent was given. Although, it allows that processing can be done for the purpose incidental to the actual purpose for which the consent was given. We'd have to extensivelyrelyupontheprecedentsfromtheEuropeanandUScourtstoanalyzethe court's interpretation ofthepurposelimitation principle. However,it is highly likely thatthecourtswillfollowtheestablishedprinciplesfromthesejurisdictions.TheBill in clear terms incorporates the principle of data minimization and provides,

> *forthepurposeconsentedtobythedataprincipalorwhichisincidental toorconnectedwithsuchpurpose,andwhichthedataprincipalwould reasonablyexpectthatsuchpersonaldatashallbeusedfor,having*

[472]KSPuttaswamyv.UnionofIndia,(2017)10SCC01, 132.

regard to the purpose, and in the context and circumstances in which the personal data was collected[473].

Further,thebill provides "*thepersonal data shallbecollectedonlyto theextent that isnecessaryforthepurposesofprocessingofsuchpersonaldata*[474]."Theprovisions do promise a data protection regime that would give to individuals complete autonomy of deciding by whom will their data be processed, the purpose for which theirdatashallbeprocessed.However,asweshallnoteintheupcomingsection,this benign beginning doesn't live up to the promise that it makes to the citizens.

5.6.1.2 StorageLimitation Principle

Theproposedbillincorporatesthestoragelimitationprincipleaswellandplacesupon the data fiduciaries an obligation of not retaining the personal data after the completionofthepurposeforwhichitwascollected[475].AparallelbetweentheGDPR and the present regulation can be drawn to suggest that the Indian data protection regimeisallsettofollowtheEuropeanmodelasfarasthedataprocessingbythedata anddataautonomyisconcerned.Although,timewilltellhowthecourtsinIndiawill interpret these principles, a close look at the principle of data autonomy and informationalself-determinationrecognizedinPuttaswamymaybehelpfulingiving an insight into the importance of storage limitation principle. It is submitted that as far as the obligations of the data controllers are concerned, the proposed Indian law appears to be in synergy with the global best practice.

5.7 Element of Consent and Processing of Data Without Consent

Element of consent is the sine qua non of every robust data protection regime. The GDPR contains a very limited definite set of grounds in which the data can be processedwithouttheconsentofthedataowner.Similarly,intheUnitedStatesas

[473]ThePersonalDataProtectionBill,§5(b),*supra*note 47.
[474]ThePersonalDataProtectionBill,§6,*supra*note 47.
[475]ThePersonalDataProtectionBill,§9(4),*supra*note47.

well, as we have noticed earlier, the grounds for processing data without the consent are extremely limited. On the other hand, the IT Act 2000 sends this principle for a toss and there is no requirement of consent at all, when the processor is the government.However,whiletheproposedActdoesinculcatetheprincipleofconsent, there are few points of concern. The Section 11 of the proposed bill is based on the principleofdataautonomyasrecognizedbytheSupremeCourtinKSPuttaswamy.[476] Itbarstheprocessingofpersonaldataexceptwhentheconsentforthesamehasbeen validly obtained by the data processor. The provision delves in the details as to how and when can the personal data be processed with the consent and the manner and mediuminwhichsuchconsentissupposedtobeobtained.Theprovisionplacesthe

[476]"ThePersonalDataProtectionBill,§11,*supra*note 47.

(1) The personal data shall not be processed, except on theconsent given by the data principal at the commencement of its processing.

(2) Theconsentofthedataprincipalshallnotbevalid,unlesssuchconsentis—

(a) free,havingregardtowhetheritcomplieswiththestandardspecifiedundersection14oftheIndian Contract Act, 1872;

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific,having regardtowhether thedataprincipalcandeterminethe scope of consent inrespect of the purpose of processing;

(d) clear,havingregardtowhetheritisindicatedthroughanaffirmativeactionthatismeaningfulina given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable totheeasewithwhichconsentmaybegiven.Restrictiononretentionofpersonaldata.Accountability of data fiduciary. Consent necessary for processing of personal data. Quality of personal data processed. 9 of 1872

(3) Inadditiontotheprovisionscontainedinsub-section

(2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained— (a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;

(b) incleartermswithoutrecoursetoinferencefromconductinacontext; and

(c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.

(6) Where the data principalwithdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal."

burden of proving that a valid consent for processing of data was obtained, entirely upon the data fiduciary. Also, the text of section 11 in clear terms specifies that the data fiduciary is under an obligation to inform the data subject about the purposefor whichthedataisbeingprocessedandbarsenjoymentofanygoods,servicesandlegal right conditional upon such consent of processing.An exhaustive analysis of the section11oftheproposedbilldoesindicatethatthelegislationdoespromiseadequate ample protection to the citizens as far as their control on their data is concerned. However,thebenignbeginningsanchoredaroundtheconceptofconsentdocometo a shocking end in the very next provision. The rights accorded to the individuals in the private domain are on the lines of protection accorded to data subjects in the GDPR.,howeverthingsdotakeadisappointingturnwhenoneanalyzestheprovisions where the data can be processed without the consent of data subjects.

5.7.1 Grounds for Processing of Personal Data Without Consent

Itissubmittedthat anexpressthreatofliabilityofthelegal consequences arisingout ofthewithdrawaldoesn'tinanywayamountto"freeconsent."Onecan'tbeexpected to make a free choice of withdrawal of consent with the sword of litigation hanging over their head. The Personal Data Protection Bill, 2019 ought to have taken into consideration,theunderlyingmeaningoftheterm"liableforalllegalconsequences" whichwouldhaveaneffectofputtingthedataprincipalintoaconstantthreatoflegal repercussions. While, it is not being suggested that the data principal should be able to withdraw their consent abruptly without any genuine reasons, to put the interests ofotherstakeholderinjeopardyoutofmalafidereasonsbutitshouldbepointedout thatthebilllacksanycomprehensiveframeworkfordeterminingwhatexactlywould bea"validreason"andwhowoulddecidethevalidityofthereason.[477]Thelegislature must take into account the fact that the data principal is the sole owner of their data and theymust notbeputto peril, in rightfully deciding to withdrawtheirconsent for sharingsomething which is entirelytheirs'.It is submitted thatthelegislatureshould comeupwithamorehumanetextasfarastheconsequencesofwithdrawalare

[477] *Id.*

concerned,thetextcouldbelimitedtotheconsequencesofcontractualobligationsin ordertoaccordthe scopeoffreeconsent atruemeaning.Also,thelegislatureshould laydownbroadguidelinesregulatingthemeaningof"validreason"forthe purposes of the Act.

Grounds of Processing of Personal Data Without Consent: A very succinct methodtogaugetheeffectivenessofanyDataProtectionlegislationistoanalyzethe tilt of balance of convenience in favor of the data principals. With, Consent being a cornerstone of the "informational self-determination", it acts as the most vital component of every data protection legislation[478].

In what came as a rude shock to most of the commentators in the field, the proposed a wide range of exceptions wherein the data of the individuals may be processed without obtaining their consent[479]. The Chapter titled as "Grounds for processing of personaldatawithoutconsentincertaincases."laysdownaveryextensivelistofthe grounds that prima facie appears to be very loosely defined.

> *"(a)fortheperformanceofanyfunctionoftheStateauthorisedbylaw for— (i) the provision of any service or benefit to the data principal from the State; or(ii) the issuance of any certification, licence or permitforanyactionor activityofthedata principalbytheState;(b) under any law for the time being in force made by the Parliament or any State Legislature; or(c) for compliance with any order or judgment of any Court or Tribunal in India; (d) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual;(e) to undertakeanymeasuretoprovidemedicaltreatmentorhealthservices toanyindividualduringanepidemic,outbreakofdiseaseoranyother threattopublichealth;or(f)toundertakeanymeasuretoensuresafety*

[478]JonathanMiller,S.,*HowDidYouKnowThat:ProtectingPrivacyInterestsofResearchParticipants via Certificates of Confidentiality*, 17 COLUM. SCI. & TECH. L. REV. 90, 99-103 (2015).
[479]ThePersonalDataProtectionBill,§12,*supra*note47.

of,orprovideassistanceorservicesto,anyindividualduringany disaster or any breakdown of public order[480]*."*

The provision has been describing as a traditional data grab law by a noted commentator, while Justice B N Sri Krishna himself, under whose chairmanship the recommendation of the proposed bill was prepared noted that the bill in its current form is going to turn India into an Orwellian state[481]. In the upcoming sections we shall analyze the validity of these clauses which virtually seek to deprive the individuals from their information autonomy based upon the principles espoused in KSPuttaswamy.Inordertohaveafairunderstandingofthecircustancesinwhichthe data of the individuals can be processed without their consent, a detailed analysis of the law laid down in KS Puttaswamy needs to be done.

5.7.2 Importance of Informational Self Determination

In the following analysis we shall stick to analyzing the opinions of the SC judges and the precedents that they have relied upon in order to assess the provisions of the upcoming bill. Particularly in the opinions of Justice Kaul, Justice Narimana and Justice Chandrachud, the dignity related aspects of informational self-determination were discussed extensively.

The SC has been of the o pinion that the consent of an individual is the most crucial aspectofinformationalprivacy[482].Mostnotablewastheobservationofjustice

[480]ThePersonalDataProtectionBill,§35,*supra*note47.

[481]MeghnaMandavia,"PersonalDataProtectionBillcanturnIndiainto'OrwellianState':JusticeBN Srikrishna" THE ECONOMIC TIMES, Dec 12, 2019, 11.34 AM IST https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[482]Kharak Singh v. State of UP, 1963 AIR 1295. "Citizen has a right to safeguard the privacy of his home, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent — whether truthfulorotherwiseand whether laudatory orcritical.Ifhedoesso,hewould beviolatingtheright to privacy of the person concerned and would be liable in an action for damages".

Nariman in Aadhar judgement wherein he observed that the right to control the dissemination of information is an inherent aspect of right to privacy and it is the right to data subject to be informed about the purposes for which his personal data is going to be used. He observed that:

> *"an aspect of privacy [is] the right to control dissemination of personal information. The boundaries that people establish from others in society are not only physical but also informational. There are different kinds of boundaries in respect to different relations. It is but essential that the individual knows as to what the data is being used for and with the ability to correct and amend it*[483]*."*

5.8 A Critique of Provisions of the Personal Data Protection Bill,2019 Enabling Processing of Personal Data Without Consent.

Right to Privacy is not an absolute right and the reason why every data protection legislation has got to have some exceptions.[484] The practical needs of a democracy mandate that certain aspects of right to privacy have to be diluted for the greater good. This is the reason why the robust data protection regimes prohibit the processing of data except in the lawful ways. While consent for processing the personal data of individual is one of the most common preconditions for processing, there are globally recognized exceptions wherein the data can be processed even without the consent of the individuals. However, these grounds are quite limited and are restricted to the following grounds. The GDPR provides that the data can be processed without the consent of the individuals for fulfilling their contractual obligations[485], for protecting the vital interests of the individuals[486], the legitimate

[483] KS Puttaswamy v. Union of India, (2017) 10 SCC 01, 224.
[484] *Id.*
[485] General Data Protection Regulation, Article 6 (EU 2016)
[486] *Id.*

interestsofthestate[487]andpublicinterest[488].Theregulationalsoprovidesthat*"when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard"* meaningtherebythattherecanbeonlyproportionaterestrictionsontheenforcement of the right to privacy.

The majority in Puttaswamy relied on the aspect of dignity attached to the informed consent quoted Justice La Forest, "*the use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity*[489]." The sole theme of the judgment revolves aroundtheabilityoftheindividualstohaveaninformedandmeaningfulcontrolover theirdata.Inthefollowingsectionswewillanalyzehowdotheprovisionsenshrined within the third chapter of the Bill run contrary to the theme of judgment in KS Puttaswamy and the challenges that these provisions may face in the constitutional courts in the upcoming days.

Asper,thebill personal dataoftheindividual maybeprocessed,"*under anylaw for the time being in force made by the Parliament or any State Legislature*[490]" which virtually means that the provision authorizes the state to grab the data of the individualsunderanylawthatitdecidestomakeitinfuture.Theclause"anylaw"is very wide and gives the impunity to the state to process the personal data without consent. This clause ignores the theme of the majority opinionin KSPuttaswamy or notisatopicofseparateanalysisandshallbetakenupinthenextchapter.However, herewewillrestrictthediscussiontothe"minimalimportance"accordedtotheright to informational self-determination in the legislation.

Justice Kaul had unequivocally highlighted the importance of informational privacy andattacheditthedecisionalautonomyoftheindividualwhilenotingthat,

[487]*Id.*
[488]*Id.*
[489]LYNDONMAITHER,"THE325":THESUPREMECOURTANDOURCRIMINALCODEAND ORS.
[490]ThePersonalDataProtectionBill,§12(b),*supra*note47.

"i*nformationalprivacy…doesnotdealwithaperson'sbodybutdealswithaperson's mind, and therefore recognizes that an individual may havecontrol over the dissemination of material that is personal to him.Unauthoriseduse of such informationmay,thereforeleadtoinfringementofthisright*[491].Theveryfactthatthe proposed bill creates a window for processing of personal data under "any law" that thestatemakes castseriousdoubtsabouttheefficiencyofthe dataprotectionregime that is going to come in place in India.

Unlike the European data protection regime that recognizes the aspect of consent as an inherent facet of informational autonomy, the proposed bill seeks to confine the issue of consent only to the private domain. Justice Chandrachud had also noted the European data protection regime where consent forms the basis of personal data processingwhilenotingthat,"*TheStatemustensurethatinformationisnot used<u>without theconsent ofusers</u>andthat itisusedforthepurpose andtotheextent it was disclosed.*[492]" The proposition once again highlightsthat the consent is an essential component for processing the data of the individuals.

Oneofthemostconcerningaspectsofthecurrentdataprotectionbillarethegrounds under which the personal data of an individual may be processed without their consent. On the same lines the bill proposes to give wide range of exemptions from theapplicationoftheAct asenshrinedunderchapterVIIoftheAct.Theexceptions proposed by the Act are quite broad and give widespread powers to the central governmenttoexemptanyauthorityfromtheauthorityoftheAct.Beforeanalyzing the constitutional validity of these provisions, the proposed provisions for exemptionsneedabriefanalysis.Section35oftheproposedBillprovidestoexempt any agency from the operation of the Act and provides that:

"WheretheCentralGovernmentissatisfiedthatitisnecessaryor expedient, —

[491]KSPuttaswamyv.UnionofIndia,(2017)10SCC01,224.,68.
[492]KSPuttaswamyv.UnionofIndia,(2017)10SCC01,224.,637.

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or(ii)forpreventingincitementtothecommissionofanycognizable offencerelatingtosovereigntyandintegrityofIndia,thesecurityofthe State, friendly relations with foreign States, public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as maybe specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

Explanation.: For the purposes of this section, (i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of theCodeof Criminal Procedure, 1973;(ii)theexpression "processingofsuchpersonaldata"includessharingbyorsharingwith such agency of the Government by any data fiduciary, data processor or data principal[493]".

The proposed section seeks to effectively empower the central government to allow any of its agencies to process the personal data of the individuals without any scant referencetothedoctrineofproportionalityatall.Itissubmittedthatthesewidespread exemptions will negate the very purpose of the new data protection regime in the country.

However,thePersonalDataProtectionBill,2019laysdownanextremelylonglistof cases wherein the data can be processed without the consent of the individuals. The Section12(b)providesthatpersonaldatacanbeprocessedwithouttheconsentofthe dataprincipal,"……*underanylawforthetimebeinginforcemadebytheParliament oranyStateLegislature*.[494]"Thiswouldeffectuallymeanthatthecentralandstate

[493]ThePersonalDataProtectionBill,§12(b),*supra*note47.

[494]ThePersonalDataProtectionBill,§12(b), *supra*note47.

governments will be at the liberty to process the personal data of the citizens under any law that is in force for the time being. Such wide windows for processing of personal data without the consent of the data principal will nullify the very purpose behind having a data protection legislation. If even after such a maneuver, the personaldataofthecitizenscanbeprocessedwithouttheconsent,undertheshieldof any law enacted by the central and state governments? It is submitted that the legislature should restrict the grounds for processing of personal data without the consent of the individuals to the grounds identified under the GDPR. The provisions in the present form, will not serve the cause of setting up a truly effective data protection regime in India unless the legislature gives adequate recognition to the element of consent for processing of personal data.

5.9 Sand box Clauses

The concept of Regulatory Sand Box is one of the newest features of the proposed Data Protection Bill, 2019. The bill allows the data fiduciaries which have implemented the Privacy by Design policy to create a sandbox for the purposes of encouraging innovation. Commentators have expressed serious doubts about the meaning of term "Sandbox" and the implications of its inclusion within the data protectionbill[495].While,theconceptofSandboxmightbeanewentranttotheIndian domain of data protection, it is a well-known concept in the arena of financial regulators[496]. The term regulatory sandbox is used todenote a safe haven that would encourage research and innovation to find out the ways in which new methods for complyingwiththelegislativerequirementscanbegenerated.Usually,thesandboxes

[495] Cheng-Yun Tsang,From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech, 2019 U. ILL. J.L. TECH. & POL'Y 355, 356-359 (2019).

[496]Regulatory Sandboxesin DataProtection:ConstructiveEngagementand InnovativeRegulation in PracticeCIPL,CENTREFORINFORMATIONANDPOLICYLEADERSHIP,2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_constructive_engagement_and_innovative_regulation_in_practice8_march_2019_.pdf.

do have a specific objective to achieve such as in case of data protection they might refer to "*innovations regarding more secure process of data processing*[497]" etc.

However,whiletherationalebehindtheSandboxclausemaybebenign,theproposed bill doesn't contain the guidelines that would govern the methods that will guide the implementation of these suggestions. Indian legislature could take a leaf from the approach of jurisdictions like Singapore and Finland[498]. It is submitted that the Proposed Bill doesn't take into considerations, the apprehensions raise by TRAI recommendations about the possible abuse of the data obtained through the sand box[499]. It is submitted that the legislature should take into account these threats and provide for a regulatory framework governing the data sandboxes. The provision in thecurrentformprovidesthat,"*TheAuthorityshall,forthepurposesofencouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox*[500]".

Itissubmittedthattheprovisionissilentuponthevitalaspectsofthedatasandboxes suchasthemechanisms,accessandrequirementofsettingupofdatasandboxesfind no mention in the bill. Following are some of the risks that are inherently associated with the data sandboxes.

- Allowing the companies to set up data sandboxes to create anonymous data may be instrumental in clogging the investments in the digital arena.
- The data aggregation and possibility of reversibility of the anonymisation process may open up avenues for profiling and mass surveillance.

It is submitted that the bill lays down detailed guidelines relating to the sandbox do clearthesubstantiatedapprehensionsofcloggininvestmentsandenablingprofiling.

---

[497] *Id.*

[498] *Supra*note165.

[499] See,TRAIRecommendationsonPrivacy,SecurityandOwnershipoftheDataintheTelecom Sector, TELECOM REGULATORY AUTHORITY OF INDIA, 52 2018, https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

[500] ThePersonalDataProtectionBill,§40,*supra*note47.

5.10 Data Protection Authority

Thedataprotectionauthoritiesinmostofthedevelopeddataprotectionregimearean indispensableaspectofprotectionofdataprivacy andimplementationofregulations under the regime[501]. An independent data protection authority is the most important aspect of the data protection framework in any jurisdiction and thus it was expected thatcreationofatrulyindependentdataprotectionauthoritywouldbethemostcrucial aspect of the data protection legislation. It is an established principle that "*the independence of the national regulatory authorities should be strengthened in order to ensure a more effective application of the regulatory framework and to increase their authority and the predictability of their decisions*[502]." Recently, the CJEU, in EuropeanCommissionv.Austria[503],retreatedtheimportanceoftheindependenceof the data protection authority while observing that the data protection authorities, "*mustenjoyanindependenceallowingthemtoperformtheirdutiesfreefromexternal influence."* The very foundation of a genuinely benign data protection legislation is the creation of a regulatory authority that is independent enough to implement the envisagedprovisions.While,independenceisaverysubjectiveconcept,thefollowing extract from the explanatory report optimally highlights the aspects of independence[504].

> "*Anumberofelementscontributetosafeguardingtheindependenceof the supervisory authority in the exercise of its functions. These could includethe composition of theauthority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions,theallocationofsufficientresourcestotheauthorityorthe*

[501]GREENLEAF,G.,ASIANDATAPRIVACYLAWS:TRADEANDHUMANRIGHTS PERSPECTIVE 212 (1st ed. 2014).

[502]Supraat218.

[503]Commissionv.Austria(2005)C-147/03.

[504]AdditionalProtocoltoConvention108,ExplanatoryReport¶17(EU2018).

adoption of decisions without being subject to external orders or injunctions."

The following observations do describe in a nutshell how a data protection authority must be formed and the ways in which it must be molded to felicitate a healthy data protectionregime.Theessentialfactorsinfluencingtheofadataprotectionauthority include its composition, the staffing of the authority, the financial structure of the authority and powers of the authority. However, the data protection authority envisaged by the proposed data protection bill have come as a rude shock and they don't assimilate any of these features in the Indian scheme.

5.10.1 Powers, Functions and Independence of Data Protection Authority

TheChapter6oftheGDPRlaysdowncomprehensiveguidelinesforthecomposition, task, competence and independence of the supervisory authority. The regulation providesforadecentralizedselectionprocessandspecificallyempowersthemembers of the authority to act independently[505] by providing that:

"*The member or members of each supervisory authority shall, in the performanceof their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody*[506]".

The language of the Article forms the backbone of the independence of the DPA in the European Union. Couched in a very wide and unambiguous language, the regulation directs that the supervisory authority would be free from all kinds of externalinterferencesandwillnotbeunderanobligationtofollowinstructionsof

[505]Article52GDPR
[506]Article52(2)GDPR

anybody. Moreover, the GDPR lays down detailed provisions that would ensure the financial and infrastructural independence of the authority[507].

The BN Sri Krishna Committee had envisaged a data protection authority that is an independent regulatory body that would have enough powers and autonomy to promoteahealthydataprotectionregimeinthecountry.[508]Furtherthecommitteehad envisaged the following roles for the authority:

- Adequatepowerstomonitor,enforcetheinvestigateprivacybreaches
- Awarenessgenerationamongstthecitizensabouttheimportanceofprivacy
- Standardsettingthroughanobjective methodology

Thelegalcommentatorswereoftheopinionthatthebodymustbeindependentinthe truest sense and able enough to promote a healthier data protection regime inthe country.[509] As per the recommendations, the composition of the committee ought to have members fromall the organs of the state and adequate technical and legal expertise[510]. The selection of the board of Data Protection Authority as per the recommendation of the committee had to be made by a selection committee which wouldbeheadedbytheChiefjusticeofIndiaorhisnominee.However,theproposed dataprotectiondoesawaywithanysuchrequirementsandprovidesthattheauthority would be appointed by the central government.[511] This raises some very serious questions about the independence of the authority. Unlike the other independent authorities in India, whose selections are made by joint committee that involves the members of the opposition parties and judiciary, the board will just prove to be an extensionoftheexecutivebranch.Theproposedbillseekstogivethecentral

[507]Article52(5)GDPR

[508]WhitePaperoftheCommitteeofExpertsonaDataProtectionFrameworkforIndia,PartIVChapter 2 (2017),

https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

[509]*Id.*

[510]*Id.*

[511]ThePersonalDataProtectionBill,§45,*supra*note47.

governmentthepowertoappoint,dismissandpaythesalaryofthemembersofboard whichmeansthattheboardoftheauthorities willcompriseofnomineesofthecentral governmentitself.Howexactlywouldtheseemployeesofthegovernmentbeableto decidethatthestateiscomplyingwiththeprovisionsoftheAct?Thepowerofcentral government to recruit and dismiss the members of the authority will reduce it to a ceremonialbodyanditsexistenceshallalwaysfeatureastheblackestspotofthedata protection bill in India. The importance of having a non-partisan select committee, the nature of office and composition of the authority are the most notable aspects of independence of any regulatory authority.

> "*The guarantee of independence is, in fact, primarily assured by the procedure of nomination and removal of theofficers of the DPAs. The control over financial resources represents a second relevant element in ensuring the autonomy of supervisory authorities".*[512]

The provisions of data protection bill have blurred the hope of an independent data protection regime in India and the completely bureaucratic composition of the authority will reduce it to a mere ceremonial body and in stark defiance of the principles of natural justice, the government itself shall be adjudicating against its own potential breaches of the provisions of the data protection legislation. It is submittedthattheselectcommitteemustconsidertheseriousnessoftheindependence of the data protection authority and make the necessary changes on the lines of suggestions made by the B N Sri Krishna Committee and the existing judicial precedents from the European Union. Only then shall India be able to create a truly effective data protection regime in the long run. The present provisions that seek to extend the executive set up to the adjudicatory mechanism in the data protection regime will do a huge disservice to the cause of right to data privacy.

[512] FRA, Data Protection in the European Union: The role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II, 8 (Luxembourg Publications Office 2010).

The Supreme Court of India while criticizing the lack of an independent regulatory authority under the Aadhar Act had shed some light on the importance of an autonomous monitoring authority by noting that having a well-structured data protection authority is quintessential to any robust data protection regime. It is only under the vigil of a competent an independent data protection authority that the individuals will be able to seek remedies under the Act.

> *"Whether it is against UIDAI or a private entity, it is critical that the individual retains the right to seek compensation and justice. This would require a carefully designed structure. An independent and autonomous authority is needed to monitor the compliance of the provisions of any statute, which infringes the privacy of an individual. Afairdataprotectionregimerequiresestablishmentofanindependent authority to deal with the contraventions of the data protection framework as well as to proactively supervise its compliance[513]."*

The Supreme Court repeatedly stressed upon the importance of "independence" of the data protection authority and highlighted the nature of the office that the data protectionauthoritywouldholdinadataprotectionregime.Initsconsideredopinion, the SC observed that the role of the data protection authority would include adjudicating upon the disputes that arise in course of the data protection law. One of the reasons behind the greater emphasis on the term "independence" is the need for an autonomous body to impartially adjudicate the disputes between the state and the citizens as far as the disputes relating to the violations under the proposed law are concerned.

> *"Independent monitoring authority must be required to prescribe the standardsagainstwhichcompliancewiththedataprotectionnormsis*

[513]KSPuttaswamyv.UOI,(2019)1SCC 01.

to be measured. It has to independently adjudicate upon disputes in relation to the contravention of the law. Data protection requires a strong regulatoryframeworkto protect thebasic rights of individuals. The architecture of Aadhaar ought to have, but has failed to embody within the law the establishment of an independent monitoring authority (with a hierarchy of regulators), along with the broad principles for data protection. The independent authority needs to be answerable to Parliament"[514].

WhatthehonorableSupremeCourthadenvisagedwasatrulyindependentregulatory body that would have administrative and judicial powers and a hierarchy of regulators. It can safely be inferred from the global best practices and the understanding of the term "independent authority" of Supreme Court, the body was supposedtobeformedonthelinesofpurely autonomousbodiessuchastheelection commission, with no possibility ofinterference from the executive and legislative organsofthestate.Giventhefactthat oneof the primaryrolesofthedataprotection authority is adjudicatory, any interference on the part of the legislative or administrative organs of the state would run counter to the ethos of rule of law[515].

5.10.1.1 Structuraland Organizational Design oftheData Protection Authority

The way in which an organization is structured and the mechanisms through which itsmembersareappointed(includingthequalification,tenure,expertiseetc.),thishas amajorimpactonthewaysinwhichtheorganizationfunctions.Thevitalfactorslike autonomy and efficiency of an organization are inherently hinged to the organizationalstructureofanystatutorybody.Itisawell-establishedprincipleofthe public that the independence of the body is inversely proportional to the external influencewithintheorganization.Thisistosay,lesserthelegislativeandexecutive

[514]KSPuttuswamyv.UOI,(2019)1SCC 01.

[515] Report of the Financial Sector Legislative Reforms Commission, Government of India Volume 1 (2013), https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf. (Accessed on 07th March, 2020).

influence in the organization, greater will be its autonomy[516]. A very colossal approachtowardscreationofanindependentregulatorybodyrestsonafour-pronged pillar, namely:

- Selectionofthe topposts of thebody by anon-partisan and non-political body.
- Guaranteeing a fixed tenureofthehead ofthe body and very limitedgrounds forhis removal. The process of removal must be partial and subject to judicial review.
- Vestingthe powerof headingtheagencyto amulti-membered board.
- Ensuringthattheagencyisself-funded.

The non-interference of the other organs in the functioning, appointment of the key members of the agency, its ability to fund itself and the security of the tenure of the head of the agency are the key features of any independent and autonomous organization[517]. When the agency is able to pay its members and get the funds for investinginpolicyandresearch,withoutbeingdependentuponthegovernmentofthe day for the funds, its ability to adhere to the text of statute faithfully, increases manifolds[518].

Unfortunately,theproposedofficeoftheDataProtectionAuthoritydoesn'tadhereto any of these four-pronged pillars. Instead, it has explicitly negated all the requirements and traits of an independent and autonomous body. The first and foremostaspectisthecompositionofthebodyandthemethodofitsappointment.As already noted, the composition of the committee that appoints the heads of any regulatory agency has the most important role in shaping the characteristics of the agency. The proposed bill provides that the:

> "*TheChairpersonandtheMembersoftheAuthorityshallbeappointed bytheCentralGovernmentontherecommendationmadebyaselection*

[516] *Id.*

[517] Stephen J., *Administrative Procedures and Political Control of the Bureaucracy*, 92 AMERICAN POLITICAL SCIENCE REV 663, 663-73 (1998).

[518] GILLIANMETZGER,DESIGNINGAGENCYINDEPENDENCE219(1st ed.2011).

committee consisting of— (a) the Cabinet Secretary, who shall be Chairperson of the selection committee; (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; (c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology[519]".

The provision in current form makes the selection committee an extension of the centralgovernment. Withnojudicialmemberpresentinit,thecommitteewillsolely comprise of the civil servants on the payroll of the government of India. This would beextremelydetrimentaltothe"independent"natureoftheagency.Theveryfactthe entirebodyoftheselectioncommitteewouldconsistofgovernmentservants,makes it imperative that the appointments to the board will be political[520].

TheexclusionoftheChiefJusticeofIndiafromtheselectionpanelis anunfortunate departure from the draft bill of 2018 and it casts serious doubts about the independenceofthebody.Theauthorityisgoingtohaveadjudicatorypowersandhis selection from a panel that is headed by the servants of the government, lands up us in an extremely complex and arbitrary situation altogether. The data protection authority, by the virtue of being an appointee of the central government, can be expected to be anything but an autonomous and independent body[521]. As we had previouslydiscussed,theauthorityhasbeenmadethesolemediumthroughwhichthe individualsaresupposedtofileaseekremediesagainstthebreachofanyoftherights guaranteed by the Act. If at all, thelegislature had the actual intention of affording a robust data protection regime, the process of appointment of the members and the chairmanofthedataprotectionboardwilldono goodtothecauseofdata protection in India.

[519]ThePersonalDataProtectionBill,§42,*supra*note47.

[520]Forfactorsinfluencingtheindependenceofregulatoryagencies,See,MichaelA.Livermore, Cost- Benefit Analysis and Agency Independence, 81 U. CHI. L. REV. 609, 611-612 (2014).

[521]*Id.*

5.11 Baron Seeking Remedy: Curtailment of the Right of Data Principle

The Bill seeks to vest into the Data Protection Authority (DPA) a wide range of adjudicatory powers and administrative powers. The proposed bill bars the courts from taking the cognizance of any offense under the Act unless a complaint for the any alleged breach of the rights under the Act has been made by the Data protection Authority[522].Indoingso,thelegislaturehasputabarrierintheformofDPAbetween the judiciary and the data principal. It must be noted that the clog on institution of a suit against the breach of the rights under the proposed legislation is quite extensive and it covers the aspect of remedies of the breach as well. The proviso to the section 63(1)oftheproposedbillreadsas,"*Providedthatnoinquiryunderthissectionshall be initiated except by a complaint made by the Authority.[523]"*The provision, thus accordstothedataprotectionauthorityanexclusiverighttomakecomplaintsagainst theallegedbreachesofrightsenumeratedwithinthelaw.Itissubmittedthatanysuch provision that bars the citizens from enforcing their rights and mandatorily take recoursetoastatutorybodytofilecomplainsiscontrarytothejudicialprecedents.It ought to be highlighted that the GDPR doesn't impose any such clog on the right of the data principal to seek remedy in the courts.

It is submitted that the legislature has made an attempt to bring in the Personal Data Protection Bill, what the Supreme Court had expressly struck down in the Aaadhar Judgment[524]. Thelegislatures affair with imposition of clog on instituting of suits by the data subjects been vitiated by the judiciary in past and hopefully, the if the said provisions see the light of the day after the review by the select committee, it is extremely unlikely that it shall pass muster to the test of "non-arbitrariness[525]." It is further submitted that the proposed bill ignores the possibility of the breaches of the rightsundertheActbytheauthorityitself.Indoingso,thelegislaturehas

[522]ThePersonalDataProtectionBill,§63(1), *supra*note47.
[523]*Id.*
[524]KSPuttuswamyv.UOI,(2019)1SCC 01.
[525]*Id.*

conveniently accorded to the Data Protection Authority the status of court of record and effectually deniedtheindividuals theright to approach to court against breaches of data privacy. One may appreciate the parallels between the Section 47 of the Aadhar Act, from which the text of Section 63(1) has copied in verbatim[526]. Interestingly, the Supreme Court had struck down the Section 47 of the Aadhar Act on the grounds that it prevented the individuals from seeking legal recourse against theviolationoftheirrights.Thefactthatthesameprovisionswerestruckdownunder theActandyettheyhavebeenadoptedintheBillwithoutevenaslightestofvariation inletterandscope,doesn'treflectwelloftheintentionsofthelegislatureasfarasthe protectionofrighttoprivacyisconcerned.Theproposedprovisionsseek topushthe entire judicial machinery on the verge of irrelevance and sterility in as much as the dataprotectionisconcerned,byrestrictingtheindividualstoapproachcourtsagainst violation of rights under the proposed bill.The foreclosure of the rights of the data subjects to seek remedy against potential breaches to their right to privacy is manifestly arbitrary[527] and thus shall eventually be struck down by the honorable Supreme Court. The finder is of the opinion that the select committee should consider the inherent fallacies in the provision and take into consideration the ruling of the Supreme Court with regards to the restriction on institution of suit under the Act.

While, the proposed bill does incorporate mechanisms for the redressal of breaches ofdataandlaysdowndetailedguidelinesregardingtheremediesavailabletothedata principal in cases of violation[528], it seeks to prohibit the data principals from taking recoursetotheefficaciousremediesavailabletothem.Whiledefending,therestraint uponsuing,imposedbythesection47oftheAadharAct,theCentralgovernmenthad contended that the, the provision wasbrought in order to maintain the purity of the Aadhar scheme[529],whichwasrejectedbytheSupremeCourtbutwhatremainstobe

[526] The Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits And Services) Act, 2016, 47 NO. 18, Acts of Parliament. (India, 2019)
[527]KSPuttaswamyvUnionofIndia(2019)1SCC01,103.
[528]ThePersonalDataProtectionBill,§25(6),*supra*note47
[529]KSPuttaswamyvUnionofIndia(2019)1SCC 01,

seen is theCentral government's justification fortheinclusion ofthesameprovision in the proposed bill. Whatever argument, the central government comes up with, the far-reaching implicationsofthewordingsoftheimpugnedprovisionintheproposed billwillfallfoultoawell-establishedjurisprudenceoftheSupremeCourtofIndia[530].

Imposing obligations on the data fiduciaries to notify the possible breach of any personaldatabeingprocessedbythemtothedataprincipal,decreasesthepossibilities of infringement of right to privacy substantially. When the personal data of an individualisbreached,aninstantnotificationofsuchbreachbytheprocessoraffords the dataprincipal, achanceto takeeffectivemeasures to minimizetheconsequences of the breach[531]. The GDPR, does take into account the implications of notice of breachandthusprovidesthatthedataprocessorsmustnotifythedataprincipalsabout data breaches within 72 hours from when the breach was detected[532]. A robust data protection regime would require that the data principal is informed about the breach ofdata,evenapossibilityofbreachofdatathroughanoticewithinagiventimeframe. The notice should adequately mention the nature of the data breach and the likely consequences of such breach.

However, the provisions of the proposed Data Protection Bill, 2019 come nowhere close to these quintessential aspects of a robust data protection regime. Instead, the proposedbillpitches forapracticethatlacks objectivityfordeterminingwhetherthe breachofdatahastobenotifiedornot.TheSection25(1)oftheproposedbillprovides that, "*Every data fiduciary shall by notice inform the Authority about the breach of anypersonaldataprocessedbythedatafiduciarywheresuchbreachislikelytocause harmtoanydataprincipal.*[533]"Thiswouldmeanthatthedatafiduciarywillbeatthe libertytoprovidethenoticeaboutapossiblebreachofpersonaldatawhentheyare

[530]MinervaMillsLtd.&OrsvsUnionOfIndia,1980AIR1789,1981SCR(1)206;L.ChandraKumar vs Union Of India And Others, 1997 (2) SCR 1186

[531]BrandonFaulkner, *Hacking intoDataBreachNotificationLaws*,59 FLA. L.REV.1097,1101- 1104 (2007).

[532]GeneralDataProtectionRegulation,Article19(EU2016).

[533]ThePersonalDataProtectionBill,§25(1),*supra*note47.

of the opinion that the breach could likely cause harm to the data principal. The provisionisbasedonthepremisethatthedatafiduciaryisbestawareoftheinterests of the data principal and it is up to them to decide whether any breach of data could result into harm to the data principal or not. Moreover, even after a subjective assessment about the likelihood of hard emanating from the data breach, which in case is found to be harmful, the data fiduciary has to give a notice to the data protection authority and not the data principal. It is submitted that while there is nothing wrong with sharing the information about the breach of personal data, the legislature should keep the most important stakeholder, the data principal in loop as well. The provisions in the present form seek to restrict the notification about the breachofdatatoanonesidedaffairbydoingawaywiththenecessityofgivingnotice to the data principal. In a fair majority of the cases, the government itself is the data fiduciary and the data protection authority which is in essence a subsidiary of the central government will be the only ones kept in the loop in case of data breaches. This would imply that, "Incaseyourdatais breached by thegovernment and ifafter acase-to-casebasissubjectiveenquiry,thegovernmentcomestoaconclusionthatthe breach could cause harm to you, it will notify the government about such breach."

By keeping the Data principal out of the loop about their own data breaches and conferringthepowersofdeterminingwhetheracertainkindofbreachcanbeharmful to the rights of the data principal to a non-independent body like Data Protection Authority, the legislature intends to negate and annihilate the principle of "informational self-determination[534]."The state can't be given such a great amount of control over the determination of the nature of the breach of data. The idea of informationalself-determinationisbaseduponthepremisethattheindividualshould be afforded complete freedom to decide when to give his data for processing, which data and for what time duration to give for processing, to decide what data breach would be beneficial and what data breach could be harmful for their interest. The individualbasednotionofrighttoprivacykeepstheinterestsandchoicesofthe

[534]LathaR.Nair,DataProtectionEffortsinIndia:BlindLeadingtheBlind,4INDIANJ.L.&TECH. 19, 21-29. (2008).

individualsatthecenterofdataprotectionregimeandhencethedenialoftherightto determine the nature of breach to the data principal themselves, would amount to a departure from the court's ruling in KS Puttaswamy v. Union of India[535]. While denying the data principals, the right to be notified about the data breaches the legislatureintendstooverlooktheveryrationalebehindtherequirementofgivingthe notice about the breaches of personal data and thus snatches the ownership rights of the data principal over their data.

Thelackofanobjectiveassessmentofthecriteriai.e.harm,willgiveanincentiveto the data fiduciaries to report a far less number of data breaches and thus eventually jeopardizetherightsofthedataprincipals. In case,thegovernmentwants tobringin atrulyeffectivedataprotectionregimethatis"Protective"oftherightsofthecitizens in the truest sense, it should makeit a point to do away with all the provisions of the billthatmightputtheindividualbasednotionofrighttoprivacyinabeyance[536].Itis submitted that the legislature should leave it to the data principals to determine whetheraparticularbreachwouldbeharmfulornot.Andhence,thesection25ofthe Personal Data Protection Bill must be amended to pose an obligation upon the data fiduciaries to notify the data principals about every breach and possibility of breach ofthepersonaldata.Thiswouldreaffirmthecommitmenttosettingadataprotection regime with adequate safeguards against the violation of individual based notion of right to privacy.

Thebillseekstomandatetheconceptof"PrivacybyDesign[537]"inordertoensurethe transparencyandaccountabilityinprocessingwhichisanappreciablefactkeepingin viewtheotherprovisionsofthebillwhichappeartobefelicitatingtheevolution ofa Data Grab Regime instead of a Data Protection Regime. However, these benign provisionsseekingadequateinfrastructureandpolicytobeimplementedbythedata

[535]KSPuttaswamyv.UnionofIndia,(2017)10SCC 01.

[536] PreetiMehta,FranchisingDataProtection andE-Commerce inIndia, 3INT'LJ.FRANCHISING L.23,23-26 (2005).

[537]ThePersonalDataProtectionBill,§22(1), *supra*note47.

fiduciaries will do no good to the cause of data protection when the legislation itself givesthemawidewindowforescapingtheapplicationoftheprovisions[538].Asfaras the private data fiduciaries are concerned, some of the aspects of proposed bill do offer some signs of a half-hearted attempt on the behalf of the legislature to set up a healthy data protection regime but cases wherein the government itself is the data fiduciary, one can observe a systematic effort by the state to control the data of the individuals and deny them any effacious legal remedy against the potential breaches of data privacy[539].

As noted, the bill seeks to vest in the data protection authority, a huge range of discretionarypowersthatwillhaveadirectimpactupontherightsandobligationsof the individuals and thus it should have been imperative for the legislature to have adequate accounting mechanism within the organization to ensure a transparent regulatorymechanism.However,thebillinitspresentformdoesn'ttakeintoaccount any of these regulatory requirements. It is submitted that the lack of involvement of judiciary in appointment of the chairman and the members of the board and lack of internal accountability mechanism within the organization will reduce the data protection authority to the second caged parrot of the central government.

As discussed earlier, the legislature has sought to make the data protection authority as a media through which the data principal would seek the remedy in the court of law. While there is not even the slightest of element of independence and autonomy in the data protection authority.Even if we assume as of now that the joint select committeemakessubstantialchangesintheorganizationalstructureoftheauthority, theproposedbillhasseverelycurtailedthepowersoftheauthoritybyprovidingfora widespread interference from the central government[540].The proposed bill seeks to bringintheinterferenceofthecentralgovernmentateverystageofthedataprotection

[538]ThePersonalDataProtectionBill,§§35,91,*supra*note47.

[539]L Chandra Kumar v. Union of India,(1997) 3 SCC 261; Minerva Mills v. Union of India, AIR 1980 SC 1789.

[540]ThePersonalDataProtectionBill,§§15,86,*supra*note47.

authority[541]. Comparing the autonomy of the Supervisory Authority established by theGDPRand theoneproposedbythe DataProtectionBill,2019highlightsthefact that there is a great deal of difference in the way the two legislatures have given importancetotheneedforhavinganindependentauthoritytoadjudicatethedisputes concerning the breach of data protection rights.

Thedeathnailinthemirageoftheindependenceandautonomyofthedataprotection regimecomesintheformofmiscellaneousprovisionsoftheproposedbill.While,we have observed a systematic approach from the central government to vend indirect control over every contour of the data protection authority, the section 86 of the proposed bill sheds all the masks and the intention of the central government to control the personal data comes out wide and clear. The section 81 of the proposed bill lays down the powers of the central government to issue directions to the data protectionauthorityand theauthoritywouldbeboundbyit.Moreover,the provision in clearterms states that thedecision ofcentral government would havethe final say on the question whether a question is one of policy or not, a question which would determine if the authority is to follow such directions or not.

5.12 Data Localization

TheJusticeSrikrishnaCommitteeinitsreportaccompanyingthedraftPersonalData Protection Bill released on July 27 noted that eight of the top 10 most accessed websitesinIndiaareownedbyU.S.entities[542].Theobjectivebehindhighlightingthis statisticwastopressforthestorageofdatawithintheterritoriallimitsofIndiatohelp the law enforcement agencies. Data localisation has emerged as one of the most debatedaspectsof thedataprotectionregimealloverthe world. Thetendencyofthe sovereignnations has beento restrict thefreeflow ofdata globallyon theaccountof

[541]ThePersonalDataProtectionBill,§62,*supra*note47.

[542] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

genuine security threats. Meanwhile, some of the countries have chosen to see the imposition of restriction of free flow of data as an instrument of furthering the cause ofnationalinterestaswell[543].Datalocalisationreferstothepracticewhereinthestates require the internet intermediaries to store the data in the country where the data has itsorigin[544].Thegenesisoftheincreasingcallfordatalocalisationcanalsobetraced in the concerns of the law enforcement agencies. The BN Sri Krishna committee report had studied the drawbacks of absence of data localisation provisions in the Indian legislation and recommended that the critical data collected in India must be stored in India itself[545]. The final Personal data protection bill, retains the provision fordatalocalisationwhileallowingthe cross-bordertransferofdatawiththeconsent oftheuserandsubjecttocertainrequirements.Inthesesections,weshallanalysethe reasons why the legislature has gone soft on the issue of data localisation and what will be the implications of the data localisation in current form on the rights of the individuals, the internet intermediaries and the law enforcement agencies[546].

WhileallowingthetransferofdataoutsideIndia,thebillcategoricallymandatesthat the sensitive personal data will have to be stored in India. The logic behind the assertion of mandatory storage of data within India is "to boost" law enforcement effortstoaccessdatanecessaryforinvestigationandprosecutionofcrimes",however, thepolicycommentatorshavepreviouslyopinedthatinsistenceuponstorageinIndia couldbecounterproductiveandevenifitreapsanybenefit,thatwouldbeminimal[547].

The argument that the data localisation within the Indian territorial limits will allow the Indian law enforcement authorities to access the data collected by the US companiesisbasedonafalsepremisethatdata localisationwouldeventuallydecide

[543]EricaFraser,DataLocalisationandtheBalkanisationoftheInternet,13SCRIPTed359(2016).
[544]*Id.*
[545]*supra*note196At91.
[546]Soldatov,A.,andBorogan,I.,Russia'sSurveillanceState,WorldPolicyJournal(2013), http://www.worldpolicy.org/journal/ fall2013/Russia-surveillance,
[547]Baueret.al,TheCostsofDataLocalisation:AFriendlyFireonEconomicRecovery,ECIPE(2014), https://ecipe.org/publications/dataloc/.

who can access the data[548]. The existing law in the United State doesn't allow its companiestodisclosethepersonaldataoftheiruserstoanyforeignlawenforcement agency and the law enforcement agencies in India have to solely depend upon the cooperative bilateral agreements like Mutual legal assistance treaty to obtain any information from the US based companies[549].

It is strange that the legislature hasn't taken into account the fact that these US companies will still be governed by the provisions of the treaty and data localisation is not going to have any impact whatsoever on the ability of Indian enforcement agencies to access the data from these companies. As per the view of the author, the legislaturehasproceededwiththemandatorydatalocalisationtostrengthenitsclaim of accessing the data within the framework of the treaty.Another neglected flaw of the proposed data localisation model emanates from the fact that a major chunk of onlinefraudandotherformsofcyber-crimehasitsgenesisoutsideIndianterritory[550].

Insuchascenario,thepropositionthatdatalocalisationwillhelpthelawenforcement authorities track and investigate crime takes a blow[551].The only way in which the law enforcement agencies within India could be benefited is through the Clarifying Lawful Overseas Use of Data (CLOUD) Act as far as the companies located in the UnitedStatesareconcerned.TheActseekstoendthemonopolyofthecontrolofUS authorities over the data. However, for any such transfer of data from the US based companies,thereneeds tobeanexecutivecontract betweenthe twocountries, which

[548]Sashidhar KJ,Easing theUS-Indiadivergence on data localization,ORF DIGITAL FRONTIERS(2019), https://www.orfonline.org/expert-speak/easing-us-india-divergence-data-localisation-53256/.,

[549]*Id.*

[550]Madhulika Srikumar, Data localisation is no solution, ORF (2018) https://www.orfonline.org/research/42990-data-localisation-is-no-solution/,

[551] Dana Polatin-Reuben and Joss Wright. An internet with BRICS characteristics: Data Sovereignty and the Balkanization of the Internet, USENIX (2014), https://pdfs.semanticscholar.org/b139/318d4b752dbc6c0383775323edc5823d9449.pdf; In 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI' 14), USENIX Association(2014), https://www.usenix.org/publications/login/dec14/foc14reports.

seems highly unlikely in near future. Given the fact that the draft bill reduces the principles of "proportionality" to a mere formality in the absence of procedural safeguard to actualize them, it ishighlylikely that the data localisation will serveno purpose in as much as the law enforcement agencies powers are concerned[552].

5.12.1 Understanding Data Localisation

Theglobaldataprotectionregimealloverthe worldhaswitnessedanincreasingtrend of restricting the free flow of data across borders for several reasons. The traditional viewthattheinternetknowsnoterritorialboundarieshasbecomemoreirrelevantthan ever before. States have justified their insistence on data localisation for protecting national security, protection of rights of the individual, free and competitive market but commentators across the globe have opined against such practice.Data localisation destroys the border less character of the internet and acts as a barrier in free flow of data and possible balkanisation of the internet. The Personal data protection bill, 2019 mandates that the counties ought to store data in India itself[553].

5.12.1.1 Protectionofthefundamental rightsoftheindividuals

Oneofthemostbeneficialaspectsofthedatalocalisationprovisionscanbetracedin their ability to strengthen the right to privacy of the individuals within the constitutional scheme of their own country[554]. Ever since the Snowden and Cambridge analytical leaks, the concerns regarding the adequateness of security of datain foreign jurisdictions havegainedground. Theargument sounds quiterational and no country should be expected to jeopardize the interests of its citizens by allowing thetransferofdatato astatethat doesn't accord sufficient protection to the rights of the data subjects[555].

[552] 17:1,JossWright.RegionalvariationinChineseInternetFiltering.Information,Communication& Society 121-141 (2014).

[553] *Id.*

[554] *Id.*

[555] *supra*note197.

While, the PDP Bill might be infested with scores of anomalies and the SC might have failed to assess the true nature of right to privacy in the Aadhar judgment, this doesn't underscorethefact that theright to privacy has been accorded thestatus ofa fundamentalrightwithintheIndianconstitutionalschemeandthereseemsnorational reasonsasnottoinsistupondatalocalisationforguaranteeingadequateprotectionto thepersonaldataofthecitizens.Itmustbeacknowledgedthattheenforcementofthe constitutional rights requires an element of control by state actors that is severely lackingwhenthebreach iscommittedbytheauthoritiesofathirdcountryandwhere the effect of that breach is ultimately only experienced on the territory of a third country[556].

The other justification of the data localisation practices has their genesis in the Snowdenpapersthathighlightedseveralsurveillancerelatedthreatsthatemanatedue to placing of data in a foreign country. However, it is highly unlikely that the data localisation, in the present form, will have any impact on the possibility of foreign surveillance in India. The fact that the sensitive data can be transferred outside India with the permission of the central government, makes India's battle against foreign surveillance an extremely weak one[557]. Moreover, it must be noted that the data localization may instead make foreign surveillance easier by effectively sanctioning centralizationofdata.Ontheotherhand,datalocalisationislikelytofurtherthecause of domestic surveillance by giving the state a complete access to the data of the citizens at one place[558]. Given the fact that the data protection authority within the proposed bill is devoid of any judicial interference, it is unlikely that the privacy of theindividualswillbeaccordedanyprotectionagainstanevasionfromthestateitself.

[556] Benjamin Wittes, Jonah Force Hill: *The Growth of Data Localization Post-Snowden,* LAWFARE (July 21, 2014, 9:14 pm), https://www.lawfareblog.com/jonah-force-hill-growth-data-localization-post-snowden-lawfare-research-paper-series.

[557]Fordetaileddiscussiononthreatofforeignsurveillance,*See,*JonahForceHill,*TheGrowthofData Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Industry leaders*, Lawfare Research Paper Series (2014), https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

[558]Chander, A. et.al,*BreakingtheWeb:DataLocalizationvs.theGlobalInternet*,(2014),http://dx.doi.org/10.2139/ssrn.2407858.

Thedatalocalisationwillvestgreatcoercivepowerinthecentralgovernmentwhich mayinturnbeusedtoextractthepersonaldataofthecitizensfromtheorganisations as per the global precedents[559].

One of the other compelling issues that stems from mandatory data legislation requirementisthethreattofreedomofspeechandexpressionInthis era,theinternet is an undisputed platform for dissemination of information throughout the globe. Platforms like twitter and Facebook have emerged as the most popular mediums to assert the participation of an individual in the political process exercising constitutional rights[560]. However, the obligation on the part of foreign companies to storethedatacollectedthroughtheirplatforminIndiawillkeepthecitizensunderan eternalscanneroftheexistingregimeofthecountry.Thiswillhaveacolossalimpact on the right to privacy of the individuals as the central government will be able to suppress dissent. The countries with similar data localisation principles have shown in recent past the ways in which a surveillance regime can be established in the garb of data localisation.

The Russian Federal Law on data localization can be classified into two broad categories namely, the Data Localization law and the Online Content law, while the online content law specifies that the data will have to be stored within the territorial limits of Russia for six months, there is no such time limit in case of the Data Localization law. This implies that the authorities will be able to retain the personal data of the individuals for unlimited duration on the pretext of affording a greater degree of protection to the right to privacy.[561]The online content law stipulates that the, "*organizers of dissemination of information in Internet'13 must 'store on the territory of the Russian Federation information about facts related to the receipt, transmission,deliveryand(or)processingofvoiceinformation,writtentexts,images, soundsandotherelectronicmessagesofusersoftheInternetandinformationabout*

[559]*Id.*
[560]*supra*note207.
[561]*Id.*

theseusers for sixmonths.[562]"This wouldimplythat thesocial mediaintermediaries andtheonlineplatformswouldberequiredtoeitherstorethedataonthepre-existing local servers within the countries or to establish a data storage center. It would tantamounttostoringthesensitivepersonaldatawiththeseserverswhichmightlack adequatesafeguardstoprivacyandthusasaresult,shallamounttoputtingtheprivacy and the national security, both in acute jeopardy[563].

Thecompliancecostsandunderlyinguncertaintyinthelegislationwillhavemultifold ramifications on the economy of the country. With an increased volume of compliance list and additional costs of investing in local servers, the businesses all overthecountryaresettobearthebruntoftheextremelyexcessiveandstringentdata protection law in Russia[564]. Several studies have outlined that the data localization will necessarily give a blow to the GDP growth rate of the country and thus there shouldn't be any hesitation in asserting that the data localization laws are inherently detrimental to the economy[565]. Apart from the economic factor, one must also take into account the procedural barriers that the data localization principles are going to haveonthedataprocessorsinthecountry.Categorizingthedataassensitiveandnon-sensitive data is one of the most difficult tasks that would substantially increase the complianceprocedureforthestakeholders[566].Moreover,theRussiandatalocalization law applies to the persons on the ground of their citizenship, with different sets of provisions in place for protection of personal data for the non-nationals.

It is submitted the Personal Data Protection Bill, 2019, by retaining the requirement for compulsory storage within the territorial limits of India has closely adopted the Russianpracticeinabitsoftenedform.Itisunfortunatethatthelegislaturehasfailed

[562] Grata International Personal Data Protection In Russia, https://gratanet.com/laravelfilemanager/files/3/Data%20Protection%20in%20Russia%202018%20final.pdf.

[563] *Id.*

[564] Daniel Garrie and Irene Byhovsky, Privacy and Data Protection in Russia, 5(2) JOURNAL OF LAW & CYBER WARFARE 235, 253 (2017).

[565] KenbeiZhang,*IncompleteDataProtectionLaw*,15GermanL.J.1071,1072-1074(2014)..

[566] *Id.*

to appreciate the genuine concerns revolving around the negative economic impacts of data localization. In the following sections, we shall note from a brief discussion about the data protection aspects of China that that the, "justifications" of data localization in India is based upon superficial assumptions.

5.12.2 DataLocalization in China

While,theEuropeancountriesalreadydohaveanextremelyadvanceddataprotection regime in place, the countries like Russia, Brazil, China and South Africa, that have a developing data protection regime may be of great interest for the purposes of analyzingthePersonalDataProtectionBill,2019.Indiaalongwiththese4 countries isamemberofaglobalbodyknownastheBRICS.Over40%oftheworldpopulation lives in the BRICS countries and over 25% of the global GDP and thus the data protectionregimeofthemembercountriesaregoingtohavefarreachingimplications on the global data protection initiatives. This will let us have an insight in to the difference of approach between the partners of BRICS towards data protection[567].
Draft Article 2 of the Personal Information and Important Data Outbound Security Assessment Measures, provides that, "*The personal information and important data collectedandgeneratedbynetworkoperatorswithinthePeople'sRepublicofChina during operations shall be stored within the [national] territory. If the business requirements make it necessary to provide data outside of China, a security assessmentshallbecarriedoutinaccordancewiththeseMeasures*[568]".Theprovision makes a sweeping assertion that all the "personal" and "important" data which has beencollectedwithintheterritoriallimitsofChinashallbestoredwithinitsterritorial limits.Theprovision,however,leavesalimitedwindowopenforthetransferofdata outsidethecountryaftera securityassessmentismadebytheauthorities.While,the

[567] Smith, D., BRICS Eye Infrastructure Funding Through New Development Bank, THE GUARDIAN, (2013),http://www.theguardian.com/global-development/2013/mar/28/bricscountries-infrastructure-spendingdevelopment-bank.
[568] Personal Information and Important Data Outbound Security Assessment Measures, Art. 2 (China 2019).

countries like India and Russia require the localization of data that is personal and sensitive, the Chinese data protection framework makes no such stipulation[569].

The Chinese Cyber security Law provides that, "important data" has to be stored within the territorial limits of the country, while there is a well settled definition of what constitutes of personal and sensitive data (with minor variations) the term important data is an entirely new concept that can amass within its meaning every possible aspect of the personal life of the citizens.[570] The comprehensiveness of the datalocalizationrequirementmakesthecaseofChinaauniqueone.Interestingly,the previous drafts of the Cyber Security laws contained the term, "Critical Information Infrastructure" instead of the term "important data" to further broaden the scope of data that ought to be localized[571]. The extensive requirement of data localization has created fears of state surveillance amongst the foreign companies operating within China. The Article 37 of the law has garnered harsh criticism from the corporate world.[572] The stringent data localization mandates of the Chinese data protection regimewillresultintocreationofdatacentersinChinabythecompaniesbasedthere or they will have to rely upon the local data storage facilities, which might even get compromisedunderthepressureofthegovernment.Itissubmittedthattheconcerns of the "State Surveillance" by the corporates do stem from the extensiveness of the data localization norms in China and are well founded.

5.13 Brazil

ThecomparisonbetweenthedataprotectionregimesinBrazilandIndiawillaffordа true insight into the difference of approach of two "democracies" towards the commitmenttoafford protectiontothe personaldata.While,inthe previoussection,

[569] AimeeBoramYang,*ChinainGlobalTrade:ProposedDataProtectionLawandEncryption Standard Dispute*, 4 ISJLP 897, 901-909 (2018).

[570] YuxiaoDuanRenmin,China'sPrivateLawApproachtoPersonalDataProtection(2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3484725.

[571] *Id.*

[572] *Id.*

thediscussionwaslimitedtotheapproachoftwoofthemostauthoritarianstateswith regards to data sovereignty, this section will, in detail, draw a parallel between the data protection laws of India and Brazil, keeping in view the various contours of a truly robust data protection regime. Brazil, just like India is a recent entrant to the league of countries having a comprehensive data protection code. The South American countryenacteditsfirstcomprehensive dataprotectionlegislationin2018 knownas theGeneral DataProtection Law[573]. However,in orderto ensureasmooth transitionintothenewdataprotectionregime,thelegislaturedecidedtopostponethe enforceabilityofthenewlawto2020.Asaresult,thelegislaturewasabletotakeinto theaccountsomeofthefallaciesintheproposedbillsuchastheintroductionofadata protectionauthority[574].BeforetheenactmentoftheGDPL,theprivacyregimeinthe countrywashingedacrossanumberofspecificregulations,includingtheconstitution of Brazil.

The GDPL is quite broad in its approach like a lot of conservative data protection enactments all over the world and is applicable only to the data collected and processed within the territorial limits of the country and the data that has been collected for the purposes of offering goods and services to the individuals in Brazil[575].OneofthemostnotableaspectsinwhichtheBrazilianapproachtothedata protectionisdifferentfromthatoftheIndianapproachistheaspectofInformational self-determination.WhereIndia'sPersonalDataProtectionBill,2019isriddledwith the grounds in which the informational self-determination goes on a toss, Brazil has adopted a very cautious and sensitive approach while striking the right balance between the informational self-determination and public interest[576].

[573] Antonio Tavares Paes, *Privacy and Data Protection in Brazil*, 5J.L.&CYBERWARFARE225, 229-233 (2018).

[574]AmarToor,BrazilandGermanymakemovestoprotectOnlinePrivacy,butExpertsseeatroubling trend toward Balkanization, 2013, http://www.theverge.com/2013/11/8/5080554/nsa-backlash- brazil-germany-raises-fears-of-internet-balkanization/.

[575]Antonio Tavares Paes, Privacy and Data Protection in Brazil, 5 J.L.& CYBER WARFARE225, 226-230 (2017).

[576]*Id.*

At the outset, it must be mentioned that the legislation expressly mentions the objective behind its enactment and to a great extent, remains committed to it. As per the Article 2 of the GDPL, the Brazilian data protection regime is based on the principles of informational self-determination, consumer protection, respect for privacy,theprotectionofthedignityoftheindividualsandcontoursofhumanrights. It is submitted that these principles reflect a holistic commitment to data protection. In order to materialize these noble goals, the GDPL adopts an extremely wide definition of "processing" of data and states that processing of personal data would mean,"*anyoperationcarriedoutwithpersonaldata,suchascollection,production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction.*[577]" The wide definitionofprocessingofpersonaldatamakesthescopeofthelawextremelybroad.

Again, following the approach ofthe GDPR, the GDPLendorses the concept of free flow of data and doesn't fall for the mirage of data sovereignty to insist upon data localization. It doesn't require data localization in any form and it is not mandatory forthedataprocessors tostorethedataintheterritoriallimitsofBrazil[578].However, the personal data can't be transferred outside the territory of Brazil only in cases whereintherequirements laiddowninsection33oftheregulationaresatisfied.This implies that the personal data can't be transferred to a country that doesn't have the samelevelofdataprotection.However,subjecttotheguaranteebythedatacontroller to afford the same level of protection as guaranteed in the regulation, personal data canbetransferredtothosecountriesaswell[579].Theregulationadditionallylaysdown

[577]Article5(X),GDPL(Brazil)

[578]Article33, GDPL(Brazil)

[579] The guarantee may be provided in the form of in the form of: a) specific contractual clauses for a giventransfer;b)standardcontractualclauses;c)globalcorporaterules;d)regularlyissuedstamps, certificates and codes of conduct.

an extensive list of cases wherein the data can be transferred outside the country in order to reaffirm its commitment to free flow of data[580].

Unlike, the Personal Data Protection Bill,2019, the GDPL chooses to tackle the key issuessurroundingtheflowofpersonaldataoutsideonanobjectivecriterionandlays downtheguidelinesfordeterminingtheparametersthatwoulddeterminethelevelof data protection in the third country. As per Article 33 of the regulation, the data protection authority would take into account the following factors to gauge the level of data protection in the third country[581].

1. The general rules governing the data protection in the third country as regards to the cross-border transfer of data in the third country.
2. Thenatureof datathatissought to betransferred to the third country.
3. Therightsofthedataprincipalsinthecountryandtheexistingcompliancemeasures.
4. Judicialandinstitutionalguaranteesfor theprotectionofinformational privacy.

Itmaybenotedthattheregulationlaysdownfairlyobjectivecriteriafordetermining the level of protection in the third country before allowing the transfers. This would afford a better protection of personal data of the individuals even in the third countries.Whenonecontraststheprovisionwiththeitsproposed Indiancounterpart, a huge spectrum of the insensitivity of the Indian state towards the protection of personal data comes into the picture. As per the Personal Data Protection Bill, the centralgovernmentandtheDataprotectionauthoritywhichisofcourseanythingbut anindependentbodywilldecidewhetherathirdcountryaffordsanadequatelevelof protection to the personal data of the citizens.

Whilecomparing Indiawithanextremelydevelopeddataprotectionregimelikethat of Europe may not be the most rational thing to do however the same comparison withacountrythatisstillinprocessofenforcingitsfirstdataprotectionbillisthe

[580] Renato Opice Blum & Camila Rioja, *Brazil's GDPR Sanctioned*, 2 Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns. 12 (2018).

[581] *Id.*

bestparametertojudgewhatiswrongwithourapproach.Whatisitthathasprompted a democracy to enact a pro data principal data protection regime and what is the inspiration of Indianpolicymakersto deviatethe most theycould from the track of a trulyeffectivedataprotectiveregime?Acloselookatsomeofthekey aspectsof the data protection legislation in both the countries reflects a systematic approach from the Indian parliament to control the subjects of data to the greatest extent and if the needarises,tograbit,withoutevenlettingthedataprincipalhavingahintaboutitat all[582].

It is submitted that the Republic of Brazil has adopted a much more data principal centric data protection law and there appears to be no attempt on the part of the Brazilian parliament to control the data of the individuals while doing lip service to the cause of data protection, unlike India[583].The GDPL appears to be far more pragmaticinitsapproachinassessingthethreattotherightsofdataprincipalsbythe state and the private parties.

Almost every data protection regime all over the world shares a common minimum program that envisages a data protection regime that encompasses the principles of fairness, lawfulness and transparency of processing of data.

Unfortunately, or fortunately, Russia has been a global hotbed in commentaries on data localization. The country is believed to have one of the most stringent data localization requirements throughout the world. The Russian federal government amendedtheOnPersonaldatalawandbroughtinanexpressrequirementforstorage and processing of data within the territorial limits of Russia. Almost half a decade ago, Russia came up with two legislations in its data protection framework that had stringent data localization requirements. The Federal Law No. 242-FZ coupled with theFederalLawNo.97-FZsetforthalethaldatalocalizationregimeinplace[584].There

[582] *Id.*

[583] *Id.*

[584] Ilya Khrennikov. Google to visa face Russia rules, Boon to Local Data Centers, BLOOMBERG QUINT(Feb,2014),http://www.bloomberg.com/news/2014-09-25/google-to-visa-face-russia-data-rules-in-boon-to-local-operators.html.

isastrikingsimilaritybetweenthedatalocalizationprinciplesunderthePersonalData Protection Bill, 2019 and the Russian data protection law. While both India and Russia are among the most swiftly emerging economies of the world, they have categorically chosen to ignore the disastrous economic ramifications of data localization principles[585] based upon finding assumptions that data localization wouldmeanenhancednationalsecurityframeworkandgreaterprotectiontotheright to privacy of the citizens[586].

5.14 Conclusion

The Comparative analysis of the Data Protection Regime in India and the EuropeanUnion,theUnitedStatesandtheUnitedKingdomalongwithsomeof the BRICS countries has highlighted a myriad set of issues that continue to plague the Indian data protection framework. While the existing data protection regime in India is completely inapplicable to the State and its agencies even the proposed data protection regime does not provide a secure firewall against the unwarranted intrusion within the private domain of the citizens. The most pressingdifferencebetweentheapproachofthecountriesintheanalysisandthe Indiana approach can be summarised in the following points:

a) While the existing data protection regime in India comes nowhere close to the global best practices on data protection, the proposed Personal Data ProtectionBill2019doesseektobridgetheexistinggapbyadoptingthekey data protection principles.
b) However, in spite of there being apparent evidences of data breaches in Aadhar program, the Indian legislature has crafted a huge window of exemption clauses that would render the state agencies capable of intruding upon the rights of the data principals on a wide range of grounds.

[585] Daniel Garrie & Irene Byhovsky, Privacy and Data Protection in Russia, 5 J.L. & CYBER WARFARE 235, 239-40 (2017).
[586] *Id.*

c) A notable departure from the focal feature of the data protection laws of the countries included within the domain of analysis portrays an attempt on the part of the legislature to shield the agencies of the central government from beingsubjectedtotheobligationsundertheact.IncontrasttotheGDPRand the UK Data Protection Act, 2018 which offer very limited grounds of exemption to the government agencies, the proposed Indian law has very wide exemption clauses.

d) AnothersignificantdepartureoftheIndianapproachtowardsdataprotection can be traced in the enforcement mechanism of the rights conferred through the legislation. The provisions of the IT Act, 2000 and the Information Technology Rules, 2011 make the safeguards inapplicable against the state and its instrumentalities. This goes a long way in watering down the effectiveness of the Indian Data protection regime.

CHAPTER6:CONCLUSIONSANDSUGGESTIONS

6.1 Introduction

The discussions in the previous chapter has highlighted some of the key issues that undermine the prospects of India's emergence as a safe jurisdiction with regards to data protection. This chapter essentially assimilates the suggestions that may be incorporated in the proposed Personal Data Protection Bill, 2019 in order to overcome the existing short comings in the draft bill.

The study has been broadly divided into six chapters that deal with the different aspects of data protection regime in India and abroad. In order to arrive at a fair assessment of the research dissertation, the finder has purportedly classified the chapters in a manner that would pave way for an optimal understanding of the importance of a robust data protection law in the country.

The most important aspect of the research was aimed at critically analyzing the provisions of the proposed data protection bill and thus to come to arrive at the answer to the dissertation of the dissertation. After, a detailed discussion into some of the key aspects of the proposed law, the finder has come to the conclusion that the dissertationofthefinderstandsansweredinpositive,anoutcomethatwasmoreor less apparent from the discussions in all the chapters. It is without doubt, true that the Personal Data Protection Bill, 2019 fails to address some of the most pressing issues concerning the data protection laws in a free democratic society. In the upcoming sections, the finder shall category highlight the aspects of the proposed law that contribute to the conclusion of arrived by the finder with regards to the dissertation.

The preamble of any legislation is one of the most vital factors influencing its interpretationbythejudiciary.Thus,itbecomesoptimaltohaveapreamblethatis

precise and assertive about its object. The Data Protection Bill's prime objective shouldbeguaranteeingtherighttodataprivacyofthecitizensofIndiaandfostering a data protection regime that is sensitive to the remotest of the breaches to the right to privacy. The preamble must also incorporate within its fold an unequivocal commitmentfromthegovernmentagainstillegalintrusionintheprivaterealmofthe individuals with a detailed roadmap of surveillance reform. The preamble should alsotakeintotheaccountthepressingneedforcreatingawarenesswithinthecountry aboutthecontoursofrighttoprivacyandthusfelicitateaprivacyconscioussociety. It is proposed that the preamble of the Data Protection Bill, 2019 be amended as:

Thepreamblethatinpithandsubstanceincorporatestheseobjectiveswill providea greater width to the rights recognized in the legislation. It is submitted that the aspectslikefosteringadigitaleconomyandundueemphasisontheeconomicaspects of data shall do no service to the right to privacy. While, these objectives may be ancillarytoarobustdataprotectionregime,therightstoprivacymustnotbepushed tothebackseatonthepremiseoffosteringdigitaleconomy.Thepreamblemust"*call a spade a spade*" and recognize the pressing need for the surveillance reform in the country and lay down a vision for a regime that is truly protective of the right to privacy in the long run. The preamble must in unequivocal terms endorse the constitutionalnecessityofprotectingandpreservingthefundamentalrighttoprivacy and thus a need for setting up a truly independent body to enforce it.

6.2 Need for A Broader Scope of DataProtection

The second most important aspect of any data protection legislation, after the preamble, is its scope. This means to say that the extent of application of the legislation determines its effectiveness in meeting its objectives set out in the preamble of the legislation. The proposed bill omits the non-personal data and the anonymised data from the application of the provisions of the law. It is submitted that numerous real-life cases have established the fact that even the non-personal dataandtheanonymiseddatacanbecombinedtoformthepersonallyidentifiable

information. In the ageofBig Dataanalytics,wherethedata can be collected in the form of meta data which can further be processed as the personally identifiable information,suchwideexemptionstothenon-personaldatamayprovetobefatalto the prospects of the data protection regime in the country.

While it is true that the data anonymisation may substantially reduce the risk involvedinprocessingofdatabutthepossibilityofreversibilityoftheprocesscannot be ruled out altogether. Thus, it is proposed that the provisions concerning the non-personal data and sensitive data be amended as follows:

Thisdefinitionwouldtakeintotheaccountthepotentialmethodsthroughwhichthe data so anonymised may be brought to the fold of personally identifiable information.Arestricteddefinitionforcategorizingthedataasanonymiseddatawill substantiallyreducethevolumeofdatawhichmightbedesignated asnon-personal. It is also suggested that the provision of the bill proposing the sharing of the non-personal data with the central government ought to be omitted altogether. It is submitted that the provisions providing for the "Promotion of Digital Economy" be duly omitted. As previously proposed, the objective of promotion of the digital economy is not in consonance of a robust data protection regime and any emphasis on the aspect may be used by the Central government to seek huge volumes of potentially personally identifiable data on the pretext of promoting a digital economy.

The evidence of such attempts is amply reflected in the Section 91 of the proposed bill. It is suggested that the language of the section 91 is a reflection of a colorable attempt from the Central government to compel the Data Protection Authority to sharethe, "Non-personal" data for all practical purposes. The provision also asserts in no uncertain terms that the decision of the central government upon the determinativequestiononsharingofsuchdatawouldbefinal[587].Itissubmittedthat

[587]ThePersonalDataProtectionbill,§91(2019),*supra*note47.Section91initspresentformprovides that, ("(1) Nothing in thisAct shall prevent the Central Government from framing of any policy for thedigitaleconomy,includingmeasuresforitsgrowth,security,integrity,preventionofmisuse,

when genuine apprehensions are surrounding the irreversibility of the process of anonymisation, such a provision would allow the Central government with a all the state machinery at its disposal, an easy run into the right to privacy of the citizens.

Itistherebysuggestedthatthewidepowersofthecentralgovernmentregardingthe processing of the "anonymised data" be deleted. This would further include the deletionofthereferencetothenon-personaldatathroughoutthenewlaw,something which appears to be a back-channel enabler of infringement of the right to privacy. Itoughttobepointedoutthatnoneoftheprogressivedataprotectionregimesacross theworldcontainsuch blanketassertionsenablingtheStateto processany personal data,coveredundertheguiseofnon-personaldataforthepurposesofpolicymaking and better targeting of the welfare schemes and the retention of the aforementioned provisions in the final bill shall be detrimental to the very concept of a robust data protection regime in the country.

6.3 A Feeble Data Protection Authority

The data protection authority is the cornerstone of any data protection authority all over the world. One may hold the position of data protection authority in a digital society to be analogous to the election commission in a democratic society. What India, as a country which is yet at a nascent stage of its awakening as a privacy conscious nation, needed was an independent agency that would place the interests ofthedataprincipalsasthemost soleobjectiveofitsexistence.Thedataprotection authority is not just a statutory body that should act upon the whims and fancies of thegovernmentoftheday,insteadtherealobjectivebehindhavingadataprotection authorityistohaveanautonomousagencyinplacethatwouldaffordsufficient

insofarassuchpolicydonotgovernpersonaldata.(2)TheCentralGovernmentmay,inconsultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed. Explanation.—For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data. (3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed").

safeguards to the citizens against any attempts from the part of the state to infringe the right to privacy of the citizens.

Inwhatcomesasthemostunfortunateanddisappointingaspectoftheproposeddata protectionbillistheofficeoftheDataProtectionAuthority.Whatthebillenvisages isnotadataprotectionauthorityeveninteremotestsense.Theproposedauthority is just an extension ofthecentral government with no element ofindependence and accountability mechanisms in place. The following are some of the most crucial aspects of the data protection authority that the proposed bill seeks to put in place. As most of the part of the bill, the objective behind the establishment of the data protectionauthorityisquitemisplaced.Toputthingsinperspective,thebillactually does make no mention of the objective behind establishment of the authority[588] and proceeds merely by explaining the nature of the institution. It is submitted that a holistic provision about the existence of the data protection authority will set forth the ground for having a more autonomous body in place.

The provision for the establishment of a data protection authority in this form shall laythefoundationofanindependentbodythathasenoughresources,infrastructural and financial capability to pursue its objective in a truly autonomous manner. The provisions stipulating the existence of at least 3 Joint Privacy Commissioners will ensure a greater degree of transparency and accountability within the authority. At the same time, keeping in consideration the mass unawareness towards the right to privacy,aseparatecoordinateoftheAuthorityforpromotingtheimportanceofright toprivacyshallbeoptimaltotheestablishmentofarobustdataprotectionregimein

[588] The Personal Data Protection bill, § 41, *supra* note 47. Section 41 in its present form provides for the establishment of the data protection authority as, "((1) The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India. (2) The Authority referred to in sub-section (1) shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued. (3) The headoffice of the Authority shall be at such place as may be prescribed. (4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India").

the country. A separate wing of the commission for monitoring state surveillance willalsogoalong way inpreventingthestate'sintrusionwithintheprivatedomain of individuals.

6.3.1 Composition of the Data Protection Authority

Thecompositionofanyagencyisanothervitalfactorinfluencingitsfunctioningand its effectiveness. The internal structuring and the guidelines that establish an accountableframeworkwithintheorganizationhaveanindispensableroletoplayin the overall character of any agency. The proposed bill lacks the acumen of establishingsuchabodyandthecompositionprescribedbyitvalidatestheargument that the data protection authority is anything but an independent body.

1. The composition of the data protection authority undermines the need for judicial oversightinthecompositionoftheauthority.[589]Theproposedbillprovidesthatout of the six members in the commission, just one member shall be from the legal background.
2. BoththeChairpersonandthemembersoftheauthoritywillbeappointedbyaselect committee that would be comprised of just the civil servants[590]. It is absurd even to suggest that anybody that is elected by the servants of the government, who are on its payroll, shall appoint a non-partisan member to the authority which would adjudicateuponthedisputesbetweenthegovernment(whereitisthedatafiduciary) against the citizens.

[589] 1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be a person having qualification and experience in law.

[590] (2) The Chairperson and the Members of the Authority shall be appointed by the Central Governmenton therecommendation madebyaselectioncommitteeconsisting of—(a) theCabinet Secretary,whoshallbeChairpersonoftheselectioncommittee;(b)theSecretarytotheGovernment of India in the Ministry or Department dealing with the Legal Affairs; and (c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.

It is submitted that neither the composition of the board nor the composition of the selection committee appointing the members of the board represent the characteristicsofanindependentagency.TheomissionoftheChiefJusticeofIndia fromtheselectionpanelisoneofthemostworryingaspectsofthebill.Itissubmitted that the composition of the board, the qualification of the board members and the composition of the selection committee be duly amended as;

Itissubmittedthatthecompositionoftheselectioncommittee,thequalificationsof themembersandthecompositionoftheDataProtectionauthoritymustbebasedon the approach as provided in the Annexure I. This will ensure an appropriate amalgamationofthejudicialandtechnicalexpertisewithintheauthority.Moreover, a non-partisan selection committee consisting of people holding constitutional and academic positions shall ensure a greater degree of autonomy and weed out the possibilities of political interferences within the functioning of the authority.

6.3.2 Terms and Conditions of Appointment

Thenextaspectthatimpactsthefunctioningofanagencyafteritscompositionisthe terms of appointment of its top brass. An agency can't be expected to work independently if the sword of dismissal keeps on hanging over their heads. Unfortunately, the bill seeks to do exactly the same by not laying an objective standardfortheprocessremovaloftheChairmanoftheDataProtectionAuthority[591].

The bill lays down that, when any member is sought to be removed on the grounds ofhiscontinualintheofficebeingdetrimentaltothepublicinterest,oronthe

[591] (1) The Central Government may remove from office, the Chairperson or any Member of the Authority who— (a) has been adjudged as an insolvent; (b) has become physically or mentally incapable of acting as a Chairperson or member; (c) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude; (d) has so abused their position as to rendertheircontinuationinofficedetrimentaltothepublicinterest;or(e)hasacquiredsuchfinancial or other interest as is likely to affect prejudicially their functions as a Chairperson or a member. (2) No Chairperson or any member of the Authority shall be removed under clause (d) or (e) of sub-section (1) unless he has been given a reasonable opportunity of being heard.

grounds that he has acquired financial or any other interest that might impact his functioning,hewouldbegivenachancetobeheard.Thebillmakesnoreferenceas to the authorities before whom such member will be given a chance to make a representation. Gauging the approach of the legislature so far, it may safely be concluded that such hearing would be made before an entirely executive body. It is thus,submittedthatinordertoensuretheautonomyoftheauthority,thereshouldbe a well-established mechanism for removal of the members. In pursuance of this objective, the provisions providing for the removal of the members of the data protection authority be amended as;

The suggested amendments will give the members a greater degree of autonomy to dischargetheirdutiesprovidedundertheproposedAct.Thiswouldalsofulfil necessitiesofimpartingthecharacterofautonomytotheauthority.Thelastand perhapsthemostimportantaspectoftheofficeofdataprotectionauthorityfromthe function perspective is the financial and functional autonomy of the agency. Theproposedbillinthepresentformenvisagesadataprotectionauthoritythatwouldbe dependentupontheCentralgovernmentforappointmentofitsmembers,theallocationofre sources,salariesofitsmembers.Itistherebysuggestedthatthe provisions providing for the salaries of the office holders be amended as follows: Thesesuggestions,ifincorporatedwithinthefinalactwillgoalongwayinestablishing a Data Protection Authority that is autonomous and independent in the truestsense.Itissubmittedthatthedataprotectionauthorityproposedbythe PersonalDataProtectionBill,2019comesnowhereclosetotheideaofan independent data protection authority envisaged by the honorable Supreme Court. Anindependent dataprotection authority that resembles theelection commission in terms of organization and structure will be at the heart of creating an effective data protection regime in India.

6.3.3 Powers of Data Protection Authority

Aftermakingthesestructuralandorganizationalchangeswithintheinstitutionofthe Data Protection Authority, the bill should also vest in the authority, enough powers tomakeitsexistencemorerelevant.Thebill,asofnowseekstosubstantiallycurtail the powers of the Authority and confers it upon the Central government. The bill vests the power in the central government to categorize certain forms of personal data as sensitive data[592]. It may be pointed out that the Data Protection Authority, with a battery of experts having a better understanding of the nuances of data, will befarbetterplaced tocategorizecertainsectionsofdataasthesensitivedata.Thus, it is proposed that Section 15(1) of the Bill be amended as:

The Data Protection Authority, with reasons noted in writing shall, in consultation with the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data",

While,itisimportanttoconferupontheDataProtectionAuthorityadequatepowers, it is equally important to have accountability mechanisms in place to secure transparency within the organization. The bill empowers the Authority the powers of, "*inspection of any book, document, register or record of any data fiduciary*[593]." However,thebill,unlikethepreviousdraft,doesn't mandatethepublicationofsuch inspectionreports. Itissuggestedthatthefollowingprovisionsbeaddedtosecurea greaterdegreeoftransparencyandaccountabilityinthefunctioningoftheauthority. The inclusion of a mandatory provision will ensure the following;

[592](1)TheCentralGovernmentshall,inconsultationwiththeAuthorityandthesectoralregulator concerned, notify such categories of personal data as "sensitive personal data", having regard to— (a) the risk of significant harm that may be caused to the data principal by the processing ofsuchcategoryofpersonaldata;(b)theexpectationofconfidentialityattachedtosuchcategory of personal data; (c) whether a significantly discernible class of data principals may suffer significantharmfromtheprocessingofsuchcategoryofpersonaldata;and(d)theadequacyof protection afforded by ordinary provisions applicable to personal data.

[593]ThePersonalDataProtectionbill,§54(8)(c),*supra*note47

1. The data fiduciaries will be more familiar with their duties and the approach taken by the authorities while interpreting the provisions of the Act.
2. The data principals will have a better understanding of the modus operandi of thedata fiduciaries.
3. ThepracticewillimpartgreaterlegitimacytothefunctioningoftheDataProtection Authority.

Theinclusionoftheseprovisionswillbebeneficialtothedataprincipal,data fiduciaries and the Data Protection Authority at the same time.

6.4 Materializing the Principle of Informed Consent

Ithasbeenalreadyobservedthattherequirementofnoticeforprocessingofpersonal data is not a mere formality. The principle underlying the requirement of notice is based upon a rationale premise that every individual has the right to informational self-determinationandtheindividualastheownerofhisdatahastherighttodecide what happens to his data. Notice also incorporates within its fold the notion of informedconsent.However,theprovisionsoftheproposedbillignorethisaspectof notice, in non-consensual processing of data. The provision does away with the requirement of notice in cases wherein the data is processed without the consent of theindividuals ifthenoticewould prejudicethepurposeforwhich datais sought to be collected.

It is submitted that the provisions providing for the non-consensual processing of data may be completely done away with or substantially amended. Further, the provisions mandating the processing of personal data whether consensual or non-consensualbeomitted.TheChapterprovidingfor thenon-consensualprocessingof data should contain the be amended as;

The limitation of processing of data without obtaining the consent of the data principals must be limited only to these emergency cases wherein obtaining the consentofdataprincipalispracticallyimpossible.Thelegislatureshouldtakeinto

account the fact that the data principal is the true owner of their data and non-consensual processing should be resorted to only in cases of emergencies.

6.4.1 Surveillance Reforms

Every state has a genuine interest to protect its sovereignty and national security. However,theopposingnotionsofnationalsecurityandrighttoprivacyhavealways been acauseofconcernforthejurists allovertheworld.While, theSupremeCourt ofIndiarecognizedtheneedforcarvingoutexemptionsfromintheDataProtection Law, smokescreen over the scope of such exemptions has yet not been cleared. On the guidelines of ICCPR and several judgments of the European Human rights Courts, the Supreme Court of India in *Justice Puttaswamy v. Union of India*[594], adopted the doctrine of proportionality within the Indian constitutional scheme for testing thevalidityoftheacts providing fortheinfringement of the right toprivacy. Asalready,discussed,thedoctrineofproportionalityisbasedonafour-prongedtest that postulates that for infringement of the right to privacy to be proportionate and thereforeconstitutionallyvalid,theactmustbein pursuitoflegitimateaim,mustbe absolutely necessary for achieving that aim, there's shouldn't be a less infringing way to achieve the same objective, the infringement must be proportional to the threat of harm.

However, It is submitted that such wide exemptions without any prescribed mechanism dealing with the nuances of surveillance are in blatant disregard to the law laid down in Puttaswamy v. Union of India[595] for the reasons discussed earlier. It is suggested the provisions relating to the exemption clauses be completely overhauled and be replaced with a separate chapter dealing with the reforming the surveillance regime in India be added. The finder would like to propose a comprehensive framework for reforming and regulating the surveillance regime in India.

[594]K.SPuttaswamyv.UnionofIndia,(2017)10SCC 01.
[595]K.SPuttaswamyv.UnionofIndia,(2017)10SCC 01.

It is submitted that the implementation of these measures will pave the way for informational privacy within the country and thus will revamp the existing surveillance regime in India. The right to informational self-determination warrants complete control of the individuals over their data and the fact that the right to privacy has been recognized as a fundamental right, makes it even more important to accord adequate protection to informational privacy.It is submitted that the suggestedprovisionsdoincorporatewithintheirrealmthedoctrineofproportionality andthuseliminatethepossibilitiesofarbitraryintrusionsintotherighttoprivacyof theindividuals.Itissubmittedthatthewhilereforminthesurveillanceregimeisone of the most indispensable aspects of a data protection regime in India which is sensitive to the rights of the data principal, it is equally important to give due weightage to the importance of informed consent.

6.4.2 The need to foster a Privacy Conscious Regime in India

A huge volume of Indian population lives below the poverty line and almost 80 million Indian live in acute poverty. A robust data protection regime in India will remainadistantdreamifthestateapparatusdoesn'ttakeuponitselfthearduoustask of creating awareness amongst the masses about the importance of informational privacy.However,insteadofincentivizingthecultureofprivacyconsciousness,the proposed bill seeks to impose barriers in the course of redressal of infringements of rights guaranteed under the law. The Section 21(2) of the proposed bill states that, "*Forcomplyingwiththerequestmadeundersub-section(1),thedatafiduciarymay charge such fee as may be specified by regulations*[596]*."* This would imply that the dataprincipalswillhavetopayformakingrequestswhileexercisingtheirrightsover their own data, which have expressly been recognized by the proposed Act.

[596]ThePersonalDataProtectionbill,§21(2), *supra*note 47.

6.5 Baron Seeking Remedies for Breach of Rights Guaranteed under the Bill

Itis,suggestedthattheallthe provisionswithintheproposedbillthatseektocreate a barrier in the form of Data Protection Authority for enforcement of the rights recognized by the law will be deleted. If at all, the legislature deems it necessary to have a role of data protection authority in the redressal of the dispute.

This would ensurethat theadjudicatorypowersof theDataProtection Authority do not come in conflict with the constitutionally guaranteed rights of the citizens of India. Moreover, the free legal opinion from the Data Protection Authority shall ensureagreaterdegreeofawarenessabouttherighttoprivacyamongstthecommon Indians.

6.6 Need for Expansion Rights of the Data Fiduciaries

It is submitted that the provisions related to the rights of data principal may be revisited in order to do away with the unnecessary procedural barriers in the enforcement of the rights.The sections dealing with the rights of the citizens be amended as proposed:

It is submitted that the express adoption of the rights of the data principals in the widest amplitude will felicitate better protection of the informational privacy of the individuals.

The aforementioned provision shall ensure that the technicalities of the procedure don't eclipse the rights of informational self-determination. It is further suggested that the aspects of sections 19[597], 21[598] and 25[599] of the bill be suitably amended to make it easier for the data principals to get their rights enforced without procedural hurdles.Itissuggestedthattheprovisotothesection20(2)bedeleted.Theprovision seekstoplacetheonusofprovingthatthecontinuedprocessingoftheirdatawillnot bedetrimentaltothepublicinterest.Itissubmittedthatthisapproachrunscounter

[597]ThePersonalDataProtectionbill,§19,*supra*note47.
[598]ThePersonalDataProtectionbill,§21,*supra*note47.
[599]ThePersonalDataProtectionbill,§25,*supra*note47.

to the ethos of informational self-determination and thus, it is suggested that the proviso be replaced by a provision that expressly puts the onus of proving that the discontinuation of processing of data would be detrimental to public interest and jeopardize the right to information. The proposed amendments coupled with the inclusionoftheexpansionofthescopeoftherightsoftheindividualsundertheAct shall be a precursor to a meaningful data protection legislation.

6.7 The Need for A Transitional Period

India is by far one of the least privacy conscious countries in the world. The Indian awakeningintoaneraofprivacyconsciousnessisyetatanextremelynascentstage. The menace of misinformation and lack of awareness plague the transition of India into a privacy conscious society. The suggested Data Protection Law is all set to introducerevolutionarychangesinthewaysoneviewstheirdata.Asofnow,ahuge chunk of Indian population who have been at the epicentre of the digital revolution in the country have scare idea of anything known as Data protection law. It is submittedthatthedataprotectionlawisn'tjustaregulatorymechanism,insteadit's aninstrumentthatwouldaltereveryaspectofthedigitalsocietythatwelinein.Thus, itisoptimaltofirstcreateasufficientdegreeofawarenessabouttherighttoprivacy andrighttoinformationalprivacyinparticulartomarkthebeginningofameaningful dataprotectionregimein thecountry.Adataprotectionlawisn't atonicthatcan be injected into the Indian society overnight to transform the prism through which the Indian view the right to privacy.

It must be noted that no number of rights conferred upon the data principals and obligations placed upon the data fiduciaries will materialize the vision of a healthy data protection regime in India. The first step has to be the creation of awareness amongst the citizens about the aspects of informational privacy both amongst the data principals and the data fiduciaries. This is the sole reason that India needs a transition sphere which would be a sort of buffer period that would ensure the transitionofIndiafromaprivacyindifferentsocietytoadataprivacysociety.The

previousdraftbill(DataprotectionBill2018)hadacknowledgedtheneedofabuffer period that would be required for the transition of the Indian society into a privacy conscious society which would understand the need for the informational privacy. It is submitted that unless there is an awareness amongst the mass about the worth of their privacy, all the substantial provisions recognizing their rights will fall into abeyance.

Moreover,acompleteoverhaulofthe Dataprotectionregimeinacountry asvastas India,willprovetobeacauseoftheruckus.Thedraftbillhadincorporatedtheneed of a transitional phase and had included a detailed framework for the date of establishmentoftheDataProtectionAuthorityandthesunriseandsunsetclausesto ensureasmoothtransitiontothenewregime.However,thePersonalDataProtection Bill, 2019 does not contain any reference whatsoever about the buffer period that wouldenablethetransition.Itissuggestedthatthebillshouldincorporateadefinite timeframeunderwhichtheprovisionsoftheActwillcomeintoforce.Failingwhich, the data fiduciaries too might feel alot of confusion regarding the new provisions which would eventually give rise to serious problems in implementation.

It is also suggested that a clear cutoff date for implementation of the provisions of the proposed Act shall set forth a clear architectural framework for the implementation of the provisions of the law, failing which, it might take years for the law to come into force. Thus, it is suggested that the provision based upon the transitionphasebeaddedtotheproposedbill.Theprovisionmaybeonthefollowing lines;

A data protection law must not only recognize the rights of the individuals; it must provideamechanismconducivetotheenforcementofsuchrights.Thebillinpresent form gives undue emphasis to the interests of data fiduciaries as far as the rights of the data principals are concerned.

Thependulumofconveniencehasbeenswinginginfavorofthedatafiduciariesfrom the very begging of the digital revolution and the data protection regime in India should do all that is needed to place the rights of the data principal on the driving seat. The onus to prove compliance of the provisions of the proposed Act must be placed upon thedata fiduciaries and the regime should felicitatetheinvolvement of data fiduciaries in becoming more privacy conscious and thus there is a pressing needtoincentivizethecommonIndianstoenforcetheirrightswithinthelaw.While, the parliament is yet to finalize the Personal Data Protection Bill, 2019, the finder would, in the light of aforementioned analysis propose the following amendments in the proposed bill in this annexure.

6.8 Conclusion

TheChaptersummariestheoutcomeofthestudyofthepervіouschapterstosuggest arobustframeworkthatwouldlaythefoundationsofastrongdataprotectionregime inIndia.Thesuggestionsincludeamendmentstothekeyprovisionsoftheproposed data protection law so that the globally accepted data protection principles are incorporated within the India data protection regime.

- TheChapterdealswiththerationaleandjurisprudencebehindthedataprotection laws all over the world. With an impetus on the need for affording adequate protection for protecting the informational privacy, the chapter highlights the contours of an effective data protection framework.
- TheChapteralsodealswiththevariousdataprotectionprinciplesthathavebeen developed across the globe while analytically distinguishing the origin of the theme of Data Protection as an aspect of the Right to Privacy.
- Thestudyaccordedathoroughinsightintotheneedofstrikingtheperfectbalance between the need to achieve the goal of informational self-determination and meeting the needs of an increasingly digitalized world.
- The undertaken study provides the finder with an insight into the key limbs of a robust data protection regime in a democratic society. With special emphasis on the OCED Principles, the finder seeks to formulate an optimumdataprotectionmodelfortheIndianschemeintheupcomingchapters.
- The study has enabled the finder to identify the key aspects of a robust data

protection regime.

- The Comparative analysis of the Data Protection Regime in India and the EuropeanUnion,theUnitedStatesandtheUnitedKingdomalongwithsomeof the BRICS countries has highlighted a myriad set of issues that continue to plague the Indian data protection framework.
- A specific study regarding the existing data protection laws in the European Union, the United Kingdom and the United States has been undertaken to get an insight into the global bestpractices related to data protection.
- The fact that European Union already has a comprehensive data protection regimeinplaceforoverthreedecadesmakesitimperativetoundertakea detailedstudyofitsdataprotectionframeworkforpragmaticallybroadeningthe ambit of analysis on the subject.
- The assessment of the existing data protection laws in the advanced data protection regimes like the United States, the European Union was aimed at establishingabenchmarkthatwouldguidetheIndianpolicymakerswithregards to the various contours of an ideal data protection regime, of courses with necessary variations to adapt to the Indian society.
- The study of data protection laws in the BRICS countries, was made with an object of drawing a parallel between the approach of authoritarian communist regimes and the liberal democracies in data protection arena.
- The study highlighted the key aspects a robust data protection regime while effectively apprising the challenges in securing informational privacy while promoting international trade.
- TheChapteronDATAPROTECTIONREGIMEININDIANLEGALSYSTEM undertakes a detailed study of the existing legislations and judicial precedents in the field of right to privacy and data protection within the Indian scheme.
- The study highlights a myriad set of lacunas within the Indian data protection framework which is ill equipped to tackle the challenges posed to the informational privacy in the wake of intense digitalization. It also brings forth the absence of key data protection principles in the existing legislations in the country.
- The study in the chapter further highlights the pressing need to enact a comprehensive data protection code that would recognize the principle of informational self-determination at its helm.

- While the existing data protection regime in India comes nowhere close to the global best practices on data protection, the proposed Personal Data Protection Bill2019doesseektobridgetheexistinggapbyadoptingthekeydataprotection principles.
- In spite of there being apparent evidences of data breaches in Aadhar progrm, theIndianlegislaturehascraftedahugewindowofexemptionclausesthatwould

  render the state agencies capable of intruding upon the rights of the data principals on a wide range of grounds.
- A notable departure from the focal feature of the data protection laws of the countries included within thedomain ofanalysis portrays an attempt on the part of the legislature to shield the agencies of the central government from being subjected to the obligations under the act.
- TheprovisionsoftheITAct,2000andtheInformationTechnologyRules,2011 makethesafeguardsinapplicableagainstthestateanditsinstrumentalities.This goesalongwayinwateringdowntheeffectivenessoftheIndianDataprotection regime.
- The finder has also done a detailed study of the approach of the India Supreme Court towards the right to privacy in order to gauge the approach that theIndianconstitutionalcourtsaregoingtotakewithregardstotheinterpretation of the provisions of the upcoming data protection law.
- The exemption clauses in the Personal Data Protection Bill, 2019 do not adhere to the doctrine of proportionality while warranting the non-application of the provisions of the proposed law to any central agencies on absolutely wide grounds of the sovereignty of India and Public order.
- These exemptions are quite wide in their scope and application and the central government shall be able to exempt any agency from the application of the provisionsoftheActforoffenceslike,"*preventingincitementtothecommission of any cognizable offence relating to public order*.[600]"

REFERENCES:

STATUTES

- Children'sOnlinePrivacyProtectionAct,15U.S.C.6501–6505
- ElectronicCommunicationsPrivacyAct,1986(P.L.99-508).
- FairCreditReporting Act15 U.S.C.§ 1681
- FamilyEducationalRightsAndPrivacyActOf1974,20U.S.C.§ 1232g
- GeneralDataProtectionRegulation(EUGDPR), (EU)2016/679
- Health InsurancePortabilityAnd AccountabilityAct,P.L.No.104-191
- IndianContractAct,1872, No.09,Acts OfParliament,1872. (India)
- InformationTechnologyAct,2000,No. 21,ActsOfParliament,2000. (India)
- IT(Amendment)Act,2008,No.10,Acts OfParliament,2009.·(India)
- PersonalDataProtectionBill,2019,BillsofParliament,2019(India)
- TheAadhaar(TargetedDeliveryOfFinancialAndOtherSubsidies,BenefitsAnd Services) Act, 2016, No. 18, Acts Of Parliament, 2016. (India)
- VideoPrivacyProtection Act,1988Pub.L.100–618

ARTICLES

- Adriana-MariaSandru;Daniel-Mihail Sandru, *Humanitarian Law andPersonal Data Protection,* 2018 PANDECTELE ROMANE 58, 61 (2018).
- Anupam Chander & Molly Land, *United Nations General Assembly Resolution on the Right to Privacy in the Digital Age*, 53 INT'L LEGAL MATERIALS 727 735 (2014).
- Asang Wankhede, *Data Protection in India and the EU: Insights in Recent Trends and Issues in the Protection of Personal Data*, 2 EUR. DATA PROT. L. REV. 70, 73 (2016).
- Asang Wankhede, *Data Protection in India and the EU: Insights in Recent TrendsandIssuesintheProtectionofPersonalData*,2EUR.DATAPROT.L. REV. 70, 86 (2016).
- Brent Snook, Joseph Eastwood, Paul Gendreau, Claire Goggin &Richard M.Cullen,*Taking Stock of Criminal Profiling: A Narrative Review and Meta-Analysis*, 34 CRIM. JUST. & BEHAVIOR 437, 455 (2007).
- BrianGorlick,*HumanRightsandRefugees:EnhancingProtectionthrough International*

Human Rights Law, 69 NORDIC J. INT'L L. 117, 126 (2000).

- Cheng-Yun Tsang, *From Industry Sandbox to Supervisory Control Box: RethinkingtheRoleofRegulatorsintheEraofFinTech,* 2019 U. ILL. J.L. TECH. & POL'Y 355, 360 (2019).
- EricaFraser, *DataLocalisationandtheBalkanisationoftheInternet*, 13 SCRIPTED 359, 365 (2016) ID.
- Eva Fialova, *Data Portability and Informational Self-Determination,* 8 MASARYK U. J.L. & TECH. 45, 53 (2014).
- FrederikZuiderveenBorgesius,JonathanGray&MireilleVanEechoud,*OpenData, Privacy,andFairInformationPrinciples:TowardsaBalancingFramework,* 30 BERKELEY TECH. L.J. 2073 2097 (2015).
- Gillian Metzger, *Designing Agency Independence,* (2011) JOTWELL: J. THINGS WE LIKE 141, 145 (2011)
- . M. Seervai, *The emergency, future safeguards and the habeas corpus case: A Criticism,* 21 TEMP. INT'L & COMP. L. J. 103, 111 (2007).
- Hallinan,D.,2019.*Opinions·DataProtectionwithoutData:CouldDataProtection Law Apply without Personal Data Being Processed?,*5(3) EUROPEAN DATA PROTECTION LAW REVIEW 293, 299.(2019).
- JoanM.Kiel,*TheHealthInsurancePortabilityandAccountabilityAct(HIPAA) Implementation Via Case Law*, 20 J. CONTEMP. HEALTH L. & POL'Y 435, 448 (2004).
- Jonathan Miller, S.,*How Did You Know That: Protecting Privacy Interests of ResearchParticipantsviaCertificatesofConfidentiality*,17 COLUM. SCI. & TECH. L. REV. 90, 100 (2015).

  <https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F1360083042000325274>
- Joshua Warmund, *Can COPPA Work - An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act,* 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189, 210 (2000).
- JossWright.*RegionalvariationinChineseInternetFiltering.*INFORMATION, COMMUNICATION & SOCIETY 121, 123 (2014).
- Laura F. Edwards, *Rights That Made the World Right*, 102 JUDICATURE 15,

20 (2018)

- Lee A. Bygrave,*Data Protection Pursuant to the Right to Privacy in Human Rights Treaties,* 6 INT'L J.L. & INFO. TECH. 247, 246 (1998).
- Lilian Edwards, *Privacy, Security and Data Protection in Smart Cities: ACriticalEULawPerspective,*2EUR.DATAPROT.L.REV.28,40 (2016)
- Lina Jasmontaite, *European Union: The European Data Protection Supervisor (EDPS)Opinion4/2015TowardsaNewDigitalEthics,*2EUR.DATAPROT. L. REV. 93, 112 (2016).
- LokkeMoerel;*RonanTigner,DataProtectionImplicationsofBrexit,*2 EUR. DATA PROT. L. REV. 381, 388 (2016).
- Maria Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right*, 3(2) INTERNATIONAL DATA PRIVACY LAW 88, 99 (2013), <https://doi.org/10.1093/idpl/ipt004>.
- MatthiasBerberich;MalgorzataSteiner,*BlockchainTechnologyandtheGDPR -How to ReconcilePrivacyandDistributed Ledgers*, 2 EUR. DATAPROT. L. REV. 422, 431 (2016).S
- MichaelA.Livermore*,Cost-BenefitAnalysisandAgencyIndependence*,81 U. CHI. L. REV. 609, 615 (2014).
- MonikaZalnieriute,*AnInternationalConstitutionalMomentforDataPrivacyinthe times of Mass-Surveillance,* 23(2) INTERNATIONAL JOURNAL OF LAW AND INFORMATION 99, 107 (2015).
- *RightsinConflict-ReconcilingPrivacywiththePublic'sRighttoKnow,*63LAW LIBR. J. 551, 563 (1970).
- Ruth Gavison,*Feminism and the Public/Private Distinction,* 45STAN. L.REV. 1,8 (1992).
- RyanM.Calo,*AgainstNoticeSkepticisminPrivacy(andElsewhere)*,87(3) NOTRE DAME LAW REVIEW 1030, 1031
- SougataTalukdar,*PrivacyandItsProtectioninInformativeTechnologicalCompass in India,* 12 NUJS L. REV. 1, 55 (2019).
- SougataTalukdar,*PrivacyandItsProtectioninInformativeTechnological Compass in India,* 12 NUJS L. REV. 1, 11 (2019)
- Subhajit Basu, *Policy-Making, Technology and Privacy in India,* 6INDIANJ.L.&TECH.65,70 (2010).

- Susan Nevelow Mart, *The Right to Receive Information,* 95 LAW LIBR. J. 175,190 (2003).
- Tschentscher*, A.,. Privacy and Data Protection by Rules Rather than Principles.* SSRN ELECTRONIC JOURNAL 153 (2017), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2372088>.
- Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data*, 21 TEMP. INT'L & COMP. L.J. 103, 106 (2007).
- Will Thomas DeVries, *Protecting Privacy in the Digital Age*, BERKELEY TECHNOLOGY LAW JOURNAL 283, 311 (2003).
- Wilson, B., *Data Privacy in India: The Information Technology Act.*2 SSRNELECTRONIC JOURNAL 82, 88 (2010).

BOOKS

- CATHERINE MACKINNON, TOWARDS A FEMINIST THEORY OF THE STATE 322 (1989).
- CHRSTOPHER KUNAR, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 57 (2003).
- CYRUS FARIVAR, HABEAS DATA: PRIVACY VS. THE RISE OF SURVEILLANCE TECH 353 (2018).
- J BLACKMAN, 'OMNIVEILLANCE, PRIVACY IN PUBLIC, AND THE RIGHT TO YOUR DIGITAL IDENTITY: A TORT FOR RECORDING AND DISSEMINATING AN INDIVIDUAL'S IMAGE OVER THE INTERNET' 321 (2009).
- JOHNBUYERS,ARTIFICIALINTELLIGENCE:THEPRACTICALLEGAL ISSUES 110 (2018)
  - JOHNKLEINIG,THENATUREOFCONSENTINTHEETHICSOF CONSENT- THEORY AND PRACTICE (4th, Alan Wertheimer and Franklin Miller eds, 2009).
- STUART RUSSEL AND PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 233 (2009).
- V. RICHARD BENJAMINS, POMPEU CASANOVAS,JOOST BREUKER,ALDO GANGEMI, LAW AND THE SEMANTIC WEB: LEGAL ONTOLOGIES, METHODOLOGIES, LEGAL INFORMATION RETRIEVAL, AND APPLICATIONS 35 (2010).
- WALTERS, ROBERT, TRAKMAN, LEON, ZELLER,BRUNODATA PROTECTION

LAW: A COMPARATIVE ANALYSIS OF ASIA-PACIFIC AND EUROPEAN APPROACHES 514 (2019).

- WILLIAM MCGEREVAN, PRIVACY AND DATA PROTECTION LAW 421 (2016).
- WOODROWBARFIELD,UGOPAGALLO,RESEARCHHANDBOOKONLAW OF ARTIFICIAL INTELLIGFENCE 675 (2018).