PRESCRIPTIVE OR OUTCOME BASED? A COMPARATIVE ANALYSIS OF INDIA'S PERSONAL DATA PROTECTION BILL AND EUROPEAN UNION'S GDPR

Dr. Rupal Rautdesai, Professor
Symbiosis Law School Pune, Symbiosis International (Deemed University)

Ms. Sudipta Chakraborty
Distinguished Visiting Faculty,
Symbiosis Law School Pune, Symbiosis International (Deemed University)

Dr. Shashikala Gurpur, Professor & Director
Symbiosis Law School, Pune, Symbiosis International (Deemed University)

Abstract

The concern regarding privacy started with the increase in the use of advanced technology related to computers and the internet. The data and information created, sent, shared, and stored in these digital files through the advanced technologies and platforms are prone to cyber-attacks leading to breach of privacy and making sensitive personal information and data public. These concerns have led many countries to adopt data protection laws, to protect the right to privacy on one hand, and to regulate the businesses that gather, store and sell such data for commercial gains, on the other hand. The authors in the research paper have discussed privacy as a construct, then its transformation, its connotations and operation in the Information and Communication Technologies World. Further, they have discussed, compared and analysed how the issues pertaining to consent, right to be forgotten and handling of sensitive personal data have been addressed in the European Union's General Data Privacy Regulation with the Personal Data Protection Bill, 2019, of India. The authors conclude on the ever-changing concept of privacy also on how the relevant issues have been addressed either through the prescriptive or the outcome-based provisions of both the GDPR and the PDPB, 2019.

Key words: GDPR, Personal Data Protection, Privacy, Right to be forgotten, Sensitive personal data

Introduction

In the initial stages of the coronavirus pandemic there was a lot of fear in the society with respect to the spread of the infection and harmful effects to their own lives. The reaction through the constant hourly news cycles of pandemic fear mongering in all media led people to take extreme steps such as asking medical workers, recent foreign travellers to vacate their apartments from their residential society in which they stayed. In addition, there has been ostracisation of families of deceased patients and those who were recovering. Knowing well the prevalence of such attitude the authorities involved in deployment of Pune's (City in India) COVID-19 contact tracing platform should have been careful about disclosure of the positive cases of COVID-19 to the general public. However, it is reported that the lax attitude of administration resulted in revealing names, locations, contact details and medical history of the patients through a link that went viral on social media platforms for some hours. This gaffe occurred after officials inadvertently made a private Google maps link developed ironically by the Smart City Development Corporation Limited of Pune (a Special Purpose Vehicle established by Government executes projects through PPP model) open to the public for hours on 25th April 2020. Further, it has been reported that instead of admitting to the error, the officials remained indifferent stating that this will make citizens more cautious. Upon knowledge of such a breach of privacy, the authorities then took immediate measures and the link was discontinued. In their defence they stated that the link was only meant for a few officials with login and password and that they will investigate how it got leaked. A source from Pune Municipal Corporation told the news reporter that this breach occurred as security layers were not put in place before planning to launch the dashboard.[1] Nonetheless the harm had already been done. Such is the case of understanding privacy and the lackadaisical attitude of authorities, app makers, social media companies as well as the major tech players who allow such apps to collect data without any oversight or owning up to any responsibility. The case reflects the lack of transition or correlation, or mutual embeddedness of prescription of rules and executive outcome in case of a crisis such as a disaster or pandemic.

There are numerous such cases of data breach reported across the world which blatantly prejudices sensitive personal information.[2] In the recently released Global Risk report by the World Economic Forum (2019) data breaches are ranked at number 5. The technological advancements have given rise to increasing fear in relation to the privacy of data and information held in digital files. This information may be about an individual's photographs,

---

[1] Kulkarni, P. (2020). *Leak of PMC Data Spread Personal Details of Patients Over Social Media*, Pune Mirror, India, available at: https://punemirror.indiatimes.com/pune/cover-story/leak-of-pmc-data-spreads-personal-details-of-patients-over-social-media/articleshow/75396397.cms.

[2] Interpol, ASEAN CYBERTHREAT ASSESSMENT 2020, available at https://www.interpol.int/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf, See also Irwin, L. (2020), *List of data breaches and cyber-attacks in March 2020 - 832 million records breached*, IT Governance Ltd., UK.

location, conversations over various social media, emails, personal financial or banking data, educational records, health related records, information from surfing the internet, leading to know more about the nature and character of the individual. The gathering of data by companies and governments regarding individuals and its intrinsic value is quite evident from the fact that most of us receive targeted advertisements when we are viewing any internet page on mobile, tablets, laptops or personal computers. All this questions the very reality of existence of the right to privacy. Thus several nations have adopted privacy and data protection regulations to regulate the conduct of businesses and technologies that affect sensitive personal information and the right to privacy.[3] One of the most appreciated normative frameworks developed and adopted is the General Data Protection Regulation of the European Union (GDPR hereinafter) which came into effect in May 2018. While India's legislation on data protection is yet to be enacted, the Indian legislature made suitable amendments to the Information Technology Act (2000) („IT Act") to include Section 43A and Section 72A, which give a right to compensation for improper disclosure of personal information. The government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under Section 43A of the IT Act which have imposed additional requirements. However, the Rules of 2011 do not expect stringent compliance, thus their effectiveness is questionable. Recognising that the current legal framework under the Information Technology Act, 2000, and its rules is not able to keep up with the technological advancements and regulate the arena of data protection and privacy, the Personal Data Protection Bill 2019 (PDPB hereinafter) was introduced. Currently the GDPR faces a few criticisms[4] including it being cost prohibitive for many businesses, silencing free speech and expression, not being able to create trust for internet users, failing to meaningfully incorporate the role of privacy.

This paper will discuss important literature on the right to privacy for a holistic understanding of the concept; while unveiling the transformation and connotations of the right to privacy in its prescriptive form in the ICT platform. Further, it will centre on an outcome-based breach of the right to privacy such as consent, the right to be forgotten and handling of personal data. It will draw a comparison among these issues under the EU GDPR and PDPB, 2019. The authors have used a descriptive, an analytical and a comparative research methodology.

---

[3] European Union's General Data Protection Regulation, 2018; Children's Online Privacy Protection Act, 2000; California Online Privacy Protection Act, 2004; Canada's Personal Information Protection and Electronic Documents Act, 2000; Personal Data Protection Act, 2010 in Malaysia; Federal Law 13,709 General Data Protection Law, 2018 of Brazil.

[4] Layton, R. (2019). The 10 Problems of the GDPR: The US Can Learn from the EU's Mistakes and Leapfrog Its Policy. AEI Paper & Studies, 1, available at: https://www.questia.com/library/journal/1G1-582399316/the-10-problems-of-the-gdpr-the-us-can-learn-from

Privacy as a construct

The earliest probable references to the concept of privacy can be traced to the distinction between the public and the private spheres by Aristotle, the Greek philosopher. While Governmental authority can be exercised over the activities falling within the public space, the activities in the private space such as „private reflections, familial relations and self-determination" cannot be subject to it.[5]

One of the classical articles on Right to Privacy by Warren and Brandeis[6] explains how the „Right to Life" meaning has changed with time. Earlier it meant only protection against battery in various forms; liberty meant freedom from real restraint; and right to property meant security of the individual for his lands and his cattle. Later, the right to life was expanded to include man's spiritual nature, his feelings, and his intellect. Further came the right to enjoy life, the right to be let alone, the right to liberty, and the right to property comprises intangible as well as tangible property.

William Beaney in his article[7] states that „a right to privacy as a legal concept can be defined as the legally recognised freedom or power of an individual (group, association, class) to determine the extent to which another individual (group, class, association, or government) may (a) obtain or make use of his ideas, writings, name, likeness, or other indicia of identity, or (b) obtain or reveal information about him or those for whom he is personally responsible, or (c) intrude physically or in more subtle ways into his life space and his chosen activities". He highlights the problems of over-defining or under-defining the right to privacy, as over definition may affect the individual's other rights such as thought and expression, freedom of religion etc, whereas under-defining could result in claims to what is clearly laid down as right to privacy by law or through court precedents.

The Black's Law Dictionary defines the right to privacy as *„right to be let alone; the right of a person to be free from unwanted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned"*.

Article 12 of the Universal Declaration of Human Rights (UDHR) says, *„No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour and reputation."*[8] The same principle is reflected in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Article 8 of the European Human Rights Convention

---

[5] James, M. (2014), A comparative analysis of the right to privacy in the United State, Canada and Europe, *Connecticut Journal of International Law*, Vol. 29, Issue 2, page 262.

[6] Warren, S. D., & Brandeis, L. D. (1890), The right to privacy, *Harvard law review*, 193-220.

[7] Beaney, W. M. (1966), The right to privacy and American law, *Law & Contemp. Probs.*, *31*, 253.

[8] Universal Declaration of Human Rights, G.A. Res. 217A (III), art. 12, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc A/810 (Dec. 10, 1948).

(EHRC) lays down *„Everyone has the right to respect for his private and family life, his home and his correspondence"*[9].

One of the experts in Privacy law from the Law School of George Washington University, in his book writes about a woman whose dog pooped on a subway train. She refused to clean up the mess when one of the passengers requested that she did so. Another passenger took photos and put them online. This spread like wildfire and due to public shaming and embarrassment, and the „dog poop girl" dropped out of the university.[10] His book deals with issues of law, civic behaviour and capability of the technological advancements. He asks whether any act that occurs in a public place takes away the right to privacy of the parties involved in such incidents. He suggests a new definition of privacy should be considered.

In India, there is no separate statutory or constitutional provision guaranteeing the right to privacy. However the jurisprudence of various cases decided in India[11] and the most recent case of ***K. S. Puttaswamy*** (popularly also known as ***Aadhar case***), [12] in which the 9 Judges Bench of the Supreme Court of India stated that the right to privacy is core of human dignity and is intrinsic and inseparable from human being, shows the increasing significance of the right. Thus, the Supreme Court interpreted Article 21 of the Indian Constitution, which guarantees the freedom of life and personal liberty, to include the right to privacy. In this case 'Aadhaar Card Scheme' of the Central Government was challenged on the ground of collecting and compiling the demographic and biometric data of the residents of the country affecting the right to privacy.

It is important to note that in the EU legal order, the fundamental right to respect for private life recognised under Article 8 of EHRC is considered to be separate from the fundamental right of data protection under the data protection laws. Though they both may be closely related as they protect similar values that is the autonomy and human dignity of individuals, they differ in their construction and scope. The right under Article 8 of EHRC is a general prohibition regarding interference, subject to certain cases such as public interest that justify interference. The right to protection of personal data is looked at as a modern and active right which puts in place a mechanism of checks and balances whenever the data of individuals is processed by any organisation or businesses.[13]

---

[9] European Convention for the Protection of Human Rights and Fundamental Freedoms Article 8, Nov. 4, 1950, 213 U.N.T.S. 221.

[10] Solove, D. J. (2007), The future of reputation: Gossip, rumor, and privacy on the Internet, Yale University Press.

[11] Minority judgement of Justice Subba Rao in the case of Kharak Singh v. The State of U.P. (1964); R. Rajagopal v. State of Tamil Nadu (1994); PUCL v. Union of India (1997) 1 SCC 301, State of Maharashtra v. Madhukar Narayan Mardikar, (1991) 1 SCC 57

[12] K. S. Puttaswamy v. Union of India (2019) 1 SCC 1.

[13] Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018.

Transformation and connotations of the right to privacy

Privacy inherently is considered to be a normative concept, with roots in philosophical, legal, sociological, political and economic traditions.[14] Its prescription as shown already, undergo contradictions, conflict and shades of non-compliance when the state or executives emphasise outcome in different context when the technology mediates or monitors or acts as a life line with its typical inanimate nature.

Kobbi and Alexandra in their position paper[15] emphasise on examining social norms and normative expectations of privacy so that technologies that are developed for complying with privacy protection are able to satisfy the expectations of the users with regard to privacy. One of the eye-catching observations of their study was that „the choices made in design of privacy regulations may reflect expedient political or practical compromises, rather than actual individual and societal expectations". To bridge this gap between the legal and normative perspectives of privacy, they suggest that the technology must satisfy the given legal definition of privacy and simultaneously develop similar approaches to analysing whether the technology satisfies the normative expectations of its users.

Mulligan, Koopman and Doty in their paper[16] argue that privacy is transformable as per the changing technological and social conditions. They suggest „a new approach to privacy research and practical design, focussed on the development of conceptual analytics that facilitate dissecting privacy's multiple uses across multiple contexts".

Privacy is understood differently by people belonging to different generations. For example Lew McCreary[17] in his paper narrates an incident where he and his mother were watching a segment on the CNN channel, in which footage was shown, from a surveillance camera in a Wal-Mart parking lot, where a woman was smacking her child in the backseat of the car. This was shocking to both the author and his mother but for very different reasons. While the author was appalled at the woman's behaviour, the author's mother was shocked that the camera was there to witness it and its invading privacy. The author has come to accept the presence of these cameras as accessories to modern life. But the author is more like his mother, conservative, when he speaks of the younger generation who self-expose on the internet their party videos, photos etc and share them without any care, which may potentially create trouble in future in more than one way. For example, now-a-days the potential employers do a

---

[14] Nissim, K. and Wood, A. (2018), Is Privacy Privacy?, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), 20170358, p. 3.

[15] Ibid, p. 16.

[16] Mulligan, D. K., Koopman, C. and Doty, N. (2016), Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118.

[17] McCreary, L. (2008), What was privacy?, *Harvard Business Review*, *86*(10), 123-30.

social media background check of candidates and such behaviour may not be acceptable to the potential employer. Another example is that if the friends with whom it is shared have shared it further to others from where it spreads, it may become subject of laughter or memes.

There has been a debate for some time now, whether a jurisdiction must utilise the so-called **„prescriptive"** method or an **„outcome-based"** approach to achieving a particular law's objectives. Under the prescriptive approach, the government defines data protection rules and requires regulated individuals and entities to comply with those rules. Both the GDPR and the PDPB 2019 prima facie seem to have adopted the prescriptive approach. Whereas the Trump Administration in the United States have advocated the outcome-based approach whereby the government focuses on the outcomes of organisational practices, rather than defining the practices themselves.[18] Only a deeper analysis of the provisions and its implementation can unfold whether the GDPR and txePDPB 2019 are prescriptive or outcome-based.

The GDPR in Article 4(1) defines „personal data" to mean „any information relating to an identified or identifiable natural person („data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[19] In this definition the focus is on identifiability, and thus if pseudonymised or anonymised data can be reverse engineered to find out the real identity then the pseudonymisation or anonymisation may not be able to escape the claims of the right to privacy. Some of the interesting cases decided by the EU Court of Justice interpreting the term „personal data" are: ***Peter Nowak v. Data Protection Commissioner***[20] – exam scripts were held to be personal data; ***Scarlet Extended SA v Société belge des auteurs*, compositeurs et éditeurs *SCRL (SABAM)***[21] – IP (Internet Protocol) address in the hands of Internet Service Providers (ISP) was held to be personal data; ***Patrick Breyer v Bundesrepublik Deutschland***[22] - Dynamic IP address in the hands of website operators was held to be personal data.

The formerly known sensitive personal data term is now illustrated under Article 9(1) of the GDPR which deals with processing special categories of

---

[18] Schwart, P. M. and Peifer, K.-N. (2019), Structuring International Data Privacy Law, *International Data Privacy Law 21*, available at https://www.law.berkeley.edu/wp-content/uploads/2019/10/Schwartz-Intl-Data-Privacy-Law-21.pdf.

[19] https://gdpr-info.eu/art-4-gdpr/.

[20] 20th December 2017 (C-434/16) available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0434

[21] 2011, Case C-70/10, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070.

[22] 19th October 2016, Case C-582/14, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582.

personal data and includes data pertaining to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometric, health, sex life or sexual orientation.

In the PDPB, 2019, Section 3(28) defines „personal data" to mean „data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such 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"[23]. Further, Section 3 (36) of PDPB, 2019 defines „sensitive personal data" to mean „such personal data, which may, reveal, be related to, or constitute - (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15".

Consent, right to be forgotten and handling of personal data

As per Article 6(1) of the GDPR, consent is one of the lawful bases on which the data can be processed. The 5 other lawful bases are: contract, legal obligation, vital interests of the data subject or another natural person, public interest, legitimate interests pursued by a controller or a third party. It is expected that consent is freely given, specific, informed and unambiguous. Consent must be sought through an intelligible and easily understandable means, using clear and plain language. It must be taken into account whether consent has been taken on processing the personal data which may not be necessary for the performance of contract. However, in practice we observe that the data subjects often are required to provide „consent" by checking a box at the end of long, technical, and complicated terms of service agreements. Article 8 of the GDPR deals with processing data where the information services are offered directly to children, in such cases the processing would be lawful only if the child is at least 16. Member states are allowed to lower this age from 16 till 13, but not below that. Where the age of the child is below the age provided in the legislation of member countries, parental consent would be mandatory. One of the major concerns is that while the children may be good with technology and different applications on mobile phones and internet, they mostly lack the capacity to understand the terms of the service providers and thus may consent to sharing data about themselves which adults would not share. The children may be unaware of the fact that their profile and behavioural data is collected and sold to data brokers, which in turn may lead to targeted advertisements or display inappropriate content to children.

[23] Personal Data Protection Bill, 2019 (Bill No. 373 of 2019) as introduced in Lok Sabha (Lower House).

In a survey conducted in a UK primary school, wherein 32 children aged between 8 to 10 years old participated and attempted questions on 8 different scenarios where they had to decide whether the information should be kept private or not and answer the reason why. The results of this survey indicated that the children do have an understanding of privacy especially related to online safety; however the children did not have the maturity to understand that their data they shared online had inherent value and they could not distinguish between which data were to be protected and which were okay to share.[24]

Processing personal data of children is pertinent to other GDPR requirements (e.g. notices must be tailored to children; the fact that data subjects are children could tip the balance of the legitimate interests test or trigger a data protection impact assessment). One recital states that significant automated decisions should not be taken concerning children.

Conditions for a valid consent under the draft PDPB[25] include free consent under section 14 of the Indian Contract Act, 1872, informed consent under Clause 7 of the PDPB. Burden of proof regarding consent has been placed on the data fiduciary and it has to prove that the consent has been given by the data principal for processing the personal data.[26]

In India, a child is defined as someone under the age of 18. The PDPB provides for a general obligation to process personal data in a manner that protects the children's rights and in a manner that is in the best interests of children. Data fiduciaries are required to verify a child's age and obtain the consent of a parent or guardian before processing any personal data of a child. The Data Protection Authority of India is empowered to promulgate regulations that specify how this is to be done. Data fiduciaries that operate online services directed at children or process large volumes of children's data may be classified as „guardian data fiduciaries" by regulations. These guardian data fiduciaries are barred from profiling, tracking, or targeting advertising at children.

In a case even before the GDPR came into existence, in the case of ***Google Spain v. González***,[27] the Court of Justice of the European Union interpreted the EU directive 95/46 as creating a presumption that at the request of a person affected (data subject) Google must delete links to personal data from its search engine results. This case affirmed the right to be forgotten.

---

[24] Dempsey, J., Sim, G., & Cassidy, B. (2018). Designing for GDPR-Investigating Children's Understanding of Privacy: A Survey Approach. available at http://clok.uclan.ac.uk/24179/1/BHCI-2018_paper_82.pdf

[25] Clause 11 of the Personal Data Protection Bill, 2019.

[26] Clause 11(5) of the Personal Data Protection Bill, 2019.

[27] Google Spain SL and Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD) and Mario Costeja González, 13 May 2014 Case C131/12, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131; Also see https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/.

As per the GDPR, individuals shall have the right to ask for deletion of their personal data in some circumstances, for example, if data is inaccurate, or not relevant for the purpose it was collected, or if it was processed in contravention of other principles. The GDPR, however, also allows data subjects to request that personal data be deleted simply on the basis that they no longer consent to any future processing of that data and that there is no other legal basis for its processing, his principle popularly known as the „right to be forgotten" or the „right to erasure".[28] Some exceptions to these rules are provided, for example if the data are conflicting with the exercise of freedom of speech and expression, or data are important for research or maintaining in the achieves. There are some criticisms to the above that these exceptions are not well defined and left for the EU member states to elaborate in their respective statutes. Further, the fear of penalties under the GDPR may encourage technology platforms to excessive takedowns of content which may affect freedom of speech and expression of other, and such other person whose freedom of expression is affected would not really have recourse to continue to have access to information that is removed.[29]

In India, as part of chapter V on the Rights of Data Principal, under Clause 18[30], the data principle has provided the right to erasure of personal data which is no longer necessary for the purpose for which it was processed. This right includes the right to correct the inaccurate or misleading personal data, complete the incomplete personal data and updating of personal data that is out-of-date. Further Clause 9 of the PDPB 2019 casts an obligation that the data fiduciary should not retain any personal data for more than the necessary period to satisfy the purpose for which it was processed and that it should delete the personal data at the end of processing them. The personal data may be retained for a longer duration only if the data subject has provided their consent. The recent case of the ***Arogya Setu Application*** (App tracking COVID-19 patients) which was earlier made mandatory in India by the Central Government had to be toned down to being recommended as there were several concerns of it affecting the right to privacy of the individuals.

Conclusion

The data privacy and data protection landscape are still evolving as there will be further technological developments affecting how data are gathered, stored, used, analysed, shared and circulated. Merely having a constitutional fundamental right to privacy or a statutory right to data protection will not solve all the problems. Courts will be often called upon to balance the individual's right to privacy with the rights of others such as the right to information by the society. Prima facie the GDPR and the PDPB, 2019 seem to be providing for the protection of an individual's right to privacy and data protection, but fail to elaborate on the

[28] Article 17.

[29] Available at https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation

[30] Clause 18 of the Personal Data Protection Bill, 2019.

exceptions under which the right may not be exercisable. Moreover, the GDPR and PDBP 2019 lack provisions for enhanced awareness among the data subjects with respect to protection of sensitive personal data and preserving their right to privacy in a meaningful way. Any country following the data protection law must hold the child's rights as paramount, just as the GDPR and the PDPB. However, how the jurisprudence in upholding the rights of the children unfold in the EU member states and in India remains to be seen. One thing is for sure that the data fiduciaries will face challenges while designing technology used by the vulnerable such as children or beneficiary in pandemic or other crises, to meet the expectations of the GDPR and the PDPB, as it is not easy to put the technical or legal language in a plain and simple manner to children. Further, the contours between data protection and freedom of expression will continue to be contested as individuals invoke the GDPR's right to erasure. Thus, although the GDPR and PDPB 2019 seem to be prescriptive, with the gaps arising out of technology-driven context as shown above, there is a huge scope for data fiduciaries to design their technologies in a way to achieve the balance between their business interests and privacy of individuals, upholding law to serve its core purpose of justice while being outcome based.

Bibliography

1. Beaney, W. M. (1966), The right to privacy and American law, *Law & Contemp. Probs.*, *31*, 253.
2. Beaney, W. M., (1967). *The Right to Privacy and American Law*, available at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3107&context=lcp.
3. Dempsey, J., Sim, G., & Cassidy, B. (2018), Designing for GDPR-Investigating Children's Understanding of Privacy: A Survey Approach, available at: http://clok.uclan.ac.uk/24179/1/BHCI-2018_paper_82.pdf.
4. Dempsey, J., Sim, G., & Cassidy, B. (2018), Designing for GDPR-Investigating Children's Understanding of Privacy: A Survey Approach, available at http://clok.uclan.ac.uk/24179/1/BHCI-2018_paper_82.pdf.
5. Irwin, L. (2020), *List of data breaches and cyber-attacks in March 2020 - 832 million records breached*, IT Governance Ltd., UK, available at: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-march-2020-832-million-records-breached.
6. James, M. (2014), *A comparative analysis of the right to privacy in the United State, Canada and Europe*, Connecticut Journal of International Law, 2014, Vol. 29, Issue 2, page 262
7. James, M. (2014), A comparative analysis of the right to privacy in the United State, Canada and Europe, *Connecticut Journal of International Law*, Vol. 29, Issue 2, page 262.
8. Kulkarni, P. (2020), *Leak of PMC Data Spread Personal Details of Patients Over Social Media*, Pune Mirror, India, available at: https://punemirror.indiatimes.com/pune/cover-story/leak-of-pmc-data-spreads-personal-details-of-patients-over-social-media/articleshow/75396397.cms.
9. Layton, R. (2019), The 10 Problems of the GDPR: The US Can Learn from the EU's Mistakes and Leapfrog Its Policy. *AEI Paper & Studies*, 1, available at: https://www.questia.com/library/journal/1G1-582399316/the-10-problems-of-the-gdpr-the-us-can-learn-from.

10. McCreary, L. (2008), What was privacy?. *Harvard Business Review*, *86*(10), 123-30.

11. Mulligan, D. K., Koopman, C. and Doty, N. (2016), Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118.

12. Nissim, K. and Wood, A. (2018), Is Privacy Privacy?, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), 20170358 3.

13. *Patrick Breyer v Bundesrepublik Deutschland* (19th October 2016), Case C-582/14, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582).

14. Schwart, P. M. and Peifer, K.-N. (2019), Structuring International Data Privacy Law, *International Data Privacy Law 21*, available at: https://www.law.berkeley.edu/wp-content/uploads/2019/10/Schwartz-Intl-Data-Privacy-Law-21.pdf.

15. Solove, D. J. (2007), *The future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale University Press.

16. Universal Declaration of Human Rights, G.A. Res. 217A (III), Art. 12, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc A/810 (Dec. 10, 1948).

17. Warren, S. D., and Brandeis, L. D. (1890), The right to privacy, *Harvard Law Review*, 193-220, available at: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

Legislation and other:

1. California Online Privacy Protection Act, 2004.

2. Canada's Personal Information Protection and Electronic Documents Act, 2000.

3. Children's Online Privacy Protection Act, 2000.

4. European Convention for the Protection of Human Rights and Fundamental Freedoms Article 8, Nov. 4, 1950, 213 U.N.T.S. 221.

5. European Union Agency for Fundamental Rights and Council of Europe (2018), *Handbook on European data protection law*, available at: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.

6. European Union's General Data Protection Regulation, 2018.

7. Federal Law 13,709 General Data Protection Law, 2018 of Brazil.

8. Google Spain SL and Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD) and Mario Costeja González, (13 May 2014) Case C131/12, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131) (https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/)

9. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018.

10. Human Rights Watch (2018), The EU General Data Protection Regulation (https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation)

11. Interpol, ASEAN CYBERTHREAT ASSESSMENT 2020, available at https://www.interpol.int/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf.

12. Personal Data Protection Act, 2010 in Malaysia.

13. Personal Data Protection Bill, 2019 (Bill No. 373 of 2019)

14. Personal Data Protection Bill, 2019 (Bill No. 373 of 2019) as introduced in Lok Sabha (Lower House).

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Cases:

1. 2011, Case C-70/10, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070.

2. 9th October 2016, Case C-582/14, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582.

3. Clause 11 of the Personal Data Protection Bill, 2019.

4. Clause 11(5) of the Personal Data Protection Bill, 2019.

5. https://gdpr-info.eu/art-4-gdpr/(20th December 2017) (C-434/16) available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0434.

6. K. S. Puttaswamy v. Union of India (2019) 1 SCC 1.

7. Kharak Singh v. The State of U.P. AIR 1963 SC 1295.

8. Minority judgement of Justice Subba Rao in the case of Kharak Singh v. The State of U.P. (1964); R. Rajagopal v. State of Tamil Nadu (1994); PUCL v. Union of India (1997) 1 SCC 301, State of Maharashtra v. Madhukar Narayan Mardikar, (1991) 1 SCC 57.

9. *Peter Nowak v. Data Protection Commissioner* (20th December 2017) (C-434/16) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0434).

10. PUCL v. Union of India (1997) 1 SCC 301.

11. R. Rajagopal v. State of Tamil Nadu. 1994 SCC (6) 632.

12. *Scarlet Extended SA v Société belge des auteurs*, compositeurs et éditeurs *SCRL (SABAM)* (2011), Case C-70/10, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070).

13. State of Maharashtra v. Madhukar Narayan Mardikar, (1991) 1 SCC 57

Acknowledgement

1. The research presented in the paper has been done under the EU-funded Erasmus+ project EURASIA: European Studies Revitalised across Asian Universities. (Project ID: 585968-EPP-1-2017-1-BG-EPPKA2-CBHE-JP.)