International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 10-02-2022, Accepted: 25-02-2022, Published: 12-03-2022
Volume 8, Issue 2, 2022, Page No. 27-32

Draft bill on data protection: A critical analysis

Shivam Gaur
Research Scholar, Maharashtra National Law University, Nagpur, Maharashtra, India

Abstract
In pursuance to the decision of the Hon'ble Supreme Court of India in the case of K. Puttaswamy v. Union of India, a committee of ten eminent members under the chairmanship of Retd. Justice B.N. Srikrishnan was constituted by the Ministry of Electronics & Information Technology, for bridging the gap of inefficient and unconsolidated existing data protection Laws in the nation with the pace of advancement of technology and the risk of data theft and misuse. This paper attempts to analyse the Bill and the author will try to identify various provisions of the Bill which have been drafted vaguely, and thereafter will try to suggest a conclusive meaning for that particular provisions of the Bill. The Author with all his bona fide intention, will try to aid the Ministry as well as the Committee appointed in achieving the desired goal behind drafting of this Bill.

Keywords: data protection bill, privacy, data fiduciary, data principle, data processor, de-identification

Introduction

Data Protection in the European Law is defined as "Law applicable to the control of the use of information about people by those into whose hands it has come". It has been derived from the community law of the European Union which provide that member state must protect the Fundamental Rights and freedoms of natural persons, in particular their Right to privacy with respect to the processing of personal data [1] Though, the community law is not restricted to the information provided on the computer only, but with this advancement of technology in the 21st century world, web has become a principle source for the theft of data. Till now, usage of personal Data or information of citizens is regulated by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which has been made by the Central Government while exercising the powers conferred to it by clause (ob) of ss. (2) of Sec. 87 r/w Sec. 43A of the Information Technology Act, 2000 [2]. Under the 2011 rules, body corporate was held liable for compensating the Data Principle in case of any data leakage due to the negligence of corporation in maintaining the security standards while dealing with the data of the individual [3] Internet has become the omnipresent abettor for the cyber criminals. It is the need of an hour to keep the sensitive personal data of an individual like his biometric details, stored online, but the nation was not having a backing of strong law to protect the data principles against data hackers and intruders. Following this lacuna in law, Hon'ble Supreme Court of India has also played an active role in the year 2017, by pronouncing a Judgement in the case of K.S. Puttaswami v. Union of India [4] through nine judge bench, ruling that the Right to privacy is protected by the Constitution as an intrinsic part of the Right to life and personal liberty u/a 21 of the Constitution of India [5]. Further the Court also observed that 'informational privacy', or the privacy of personal data and facts, is an essential facet of Right to privacy [6].

To overcome all of these above mentioned problems and for enacting one consolidated Bill on Data protection which will seeks to protect the autonomy of individuals with respect to their personal data, specify norms of data processing by entities using personal data, and set up a regulatory body to oversee data processing activities, Ministry of Electronics & Information Technology has issued an Office Memorandum on 31st July, 2017 for constitution of a committee of experts to deliberate on a data protection framework for India [7] Committee was constituted under the chairmanship of Justice B.N. Srikrishna, Former Judge of Supreme Court of India and comprised of eight other eminent experts from various other fields of expertise. Joint secretary of the Ministry of Electronics & Information Technology was made the member convener for the committee [8]

Committee has done a sincere hard work for a period of one year and has also taken the advice from stakeholders present across the nation by conducting four public consultation meetings at different venues throughout the country, i.e., at Delhi, Hyderabad, Bengaluru, and Mumbai [9] After listening to stakeholders, ministers and various individuals, going through all the existing scattered laws on Data Protection prevalent in India, analyzing the areas for which laws must be drafted, and also after comparing situation existing in India with that of other nations, committee has well drafted a Bill comprising of 112 Articles and two Schedules and presented the same before the ministry on 27th July, 2018 [10]. The bill include the definition of the important terms, Obligation of data fiduciaries, Grounds on which personal data can be processed, differentiation between personal data and sensitive personal data, how to protect the personal data of children, rights of data principles, measures that should be adopted for transferring the personal data outside India, defining consent and what areas must be

covered in exemption from taking the consent, composition of Authorities required for implementation of these laws relating to Data protection and further to impose penalties on offenders and many more [11].

The present paper is an attempt to study and analyse the Draft of Data Protection Bill, 2018 based on the primary and secondary sources using the official reports and documents of Ministry of Electronics & Information technology, Legislative Provisions for Data Protection regime, and academic research papers in the area of Data Protection. The committee has well drafted a consolidated bill in this domain, but still some vague terminologies are being used by the experts in the language of the bill, Author will try to do complete justice to the intention of the ministry and will provide an appropriate definition to these vague terminologies.

The author argues that the real intention of the Ministry behind assigning this whole long task of drafting a consolidated bill on data protection to the committee is to bridge the gap between the incapacity of existing laws enforced in India for protecting the individual's data with the pace of advancement of technology and the advanced resources available with the cyber criminals or with data thieves. It is very difficult to find the actual accused who has committed the crime, and in case appropriate authority successfully trace the accused, there are multiple lacunas in the existing legislature for the Data Protection under which the Accused can easily escape the punishment. In the light of this assumption, the Researcher tries to analyse various provisions of the Data Protection Bill 2018, find the existing lacunas in the Bill, and will provide some suggestions to fill the gap between the intention of the ministry and the draft presented by the committee.

Characteristics of The Bill

Similar to every other Act, this Bill also start with defining the key terms used further in the Bill. Some of the terms that are defined in the Bill are Personal Data [12], Data Processor [13], Data Principal [14], Data Fiduciary [15], Consent [16], De-identification [17], Harm [18], Sensitive Personal Data [19] and many more. The personal data, as per the Bill, can be processed both by Government and by both Private entities incorporated in India as well as incorporated overseas. Data fiduciaries can only process the data of an individual after they have obtained the valid consent from the Data principle. There are some areas which are exempted by the committee from this consent taking process, including, any function of the parliament or state legislature, if required under any law or in furtherance of any Court judgement, response to any medical emergency, etc., as all these areas are in public welfare domain and therefore theory of utilitarianism is applied [20]. On the other hand, in order to process any sensitive personal data, an express consent is required by the Data Fiduciaries prior to processing the individual data [21].

Chapter II of the Bill mentions certain obligation upon the Data Fiduciaries for satisfying the dual objectives of limiting processing to the fulfilment of purposes of data principals, while maximizing gains from data processing for society at large [22] Such obligations require careful adaptation with the emergence of advanced technological world facilitated by Artificial Intelligence and machine learning. Some of the obligation proposed in the Bill are processing personal data in a fair and reasonable manner; notifying the data principle of the nature and purposes of data collection, and their rights among others; collecting only as much data as is needed for a specified purpose and not storing that data for a longer period of time; Data fiduciaries must process the data in an utmost transparent manner; and personal data being used should be relevant to the purpose for which it is used and should be accurate, complete and kept up-to-date [23]

As a universal fact we all are aware that there exist a corresponding right for every duty, and hence, certain rights are provided to the Data Principle under Chapter VI of the Bill. These rights are based on the principles of autonomy, self-discrimination, transparency and accountability so as to give individuals control over their data, which in turn is necessary from freedom in the digital economy [24] The committee has provided all such rights to Data principals under the umbrella of the Constitution of India, as certain Rights flow from the freedom of speech and expression and the Right to receive information under Article 19(1)(a) and Article 21 of the Constitution [25] Some of the Rights guaranteed to data principals under the Bill are right to obtain a summary of their personal data held with the data fiduciary; right to seek correction of inaccurate, incomplete or outdated personal data; right to have personal data transferred to any other data fiduciary in certain circumstances; right to be forgotten which allows the data principal to restrict or prevent continuing discloser of their personal data [26].

Data fiduciary has to keep one copy known as 'serving copy' of all the personal data in a server which must be situated in India [27] Bill has empowered central government with a special power of exempting some categories of personal data from this formality on the grounds of strategic interest of the state or necessity. Critical personal data shall be processed only in servers located in India [27]. Under certain broadly defined circumstances, data fiduciaries may transfer the personal data outside the country, but, except the grounds specified under sub-sec. 3 of sec. 41, under no other circumstance can a sensitive personal data which is critical be transferred outside the nation [27] Data can be transferred outside the country only after taking permission from central government or by the Data Protection Authority, *hereinafter as DPA [28]*.

Enforcement of laws is the major role-player behind the success of any legislation. A law is said to be only as good as its enforcement. After reviewing theoretical literature, gathering practical experience of other countries in enforcing data protection laws, and analyzing the experience of our own country with respect to enforcement and public comments to the white paper of the committee, a responsive regulatory framework equipped with the range of tools has been found by them to be of critical importance [28] Thereafter, the detailed discussion committee has provided for the establishment of DPA empowering it with drafting of specific regulations for all data fiduciaries across different sectors; supervise and monitor data fiduciaries; assess compliance with the bill

and initiate enforcement actions; and receive, handle and redress complaints from data principals [29] The composition of DPA must be of seven members in total, out of which one member must be the Chairperson. All the members of DPA must has a knowledge and minimum experience of ten years in the field of data protection and information technology [30] There must be a separate wing of DPA for adjudicating the matters. The adjudication wing must comprise of officers who are specialized in the area of cyber law, constitutional law, and data protection, and are also having an experience of seven years in any of the above mentioned fields [31] Aggrieved from the order of the adjudication wing, a person can file an appeal before the Appellate Tribunal which has been set up by the central Government, and in furtherance to the impugned order from the tribunal, a party can prefer an appeal to the Supreme Court [31].

The adjudicating officer under the adjudication wing of the DPA has been given the power to impose monetary penalties on infringing data fiduciaries [32] The aim of the committee is to impose such a penalty which will make it unprofitable for data fiduciary to engage in wrongful act in future and should be in proportion to the harm suffered by the data principal [33] In furtherance to the penalty, committee also recommended to impose a liability upon data fiduciary of paying the amount of compensation. Compensation amount must be paid at the first instance of very proving the infringement, so that the aggrieved data principal will receive the compensation amount due to him [35] Bill also contains the provisions for offences created in order to punish the data fiduciary for their intentional or reckless behavior [36] Penal liability for the offences is between 2-5 years of term, whereas, monetary penalty may extent to five crore rupees or two percent of its total worldwide turnover of the preceding financial year. Monetary penalty in some of the specified cases can even extent up to fifteen crore rupee or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher [37].

Way outs in the bill

Law is made for the society, either by identifying the cure for the existing problem in the society or by foreseeing that issues which can be of sociological importance in the near future, and thus provides a well-defined substantial as well as procedural solutions for those issues. Since the society is not static, no law can be perfect at any point of time, there is the scope of improvement always. With this approach, author will now try to find some loopholes in the Bill proposed by Srikrishna committee.

Data fiduciary is under the obligation to demonstrate to the DPA, and to ensure that the personal data of an individual is processed in a fair and reasonable manner in order to respect the privacy of an individual [38]. If any violation is done by the Data Fiduciary in above mentioned procedure, than he is liable to pay a penalty of four per cent of his total worldwide turnover which is further subjected to minimum of Rs. 15 crore [39]. While the bill places this obligation on all data fiduciaries, it does not specify any principles or guidelines for what constitutes a 'fair and reasonable' manner of personal data processing. This lack will hamper the fairness and will open the gates for biasness as fiduciaries generating similar type of data can get different treatment by the authority. In the absence of any guidelines, it will be unreasonable to expect the fiduciary to demonstrate compliance. Giving power to Courts and regulatory authority for defining fairness and reasonableness will have a negative impact on the transparent enforcement of Act.

Data Fiduciaries are under the obligation to inform the DPA in the event of data breach only if the breach is likely to cause harm to any data principal [40]. This ambiguity in the language of the provision implies the discretion upon the data fiduciary to determine whether there is any need of reporting a breach of data to DPA or not. Data is a very sensitive issue, importance of the data can vary from person to person. Any person can't be in the position to determine the importance of leakage of any data for someone else. It is very wide discretion given to the data fiduciary using which it can easily escape the penal as well as monetary liability.

Further, data fiduciaries are under the obligation of taking the consent of data principal by providing him an advance notice, before processing his data [41]. However, the Bill specifies certain exempted areas in which there is no need for such a consent like national security; legal proceedings; research and journalistic purposes etc [42]. Author at this point would like to raise a question of whether all these exemptions are warranted or not? Earlier under tort law, the concept of strict liability was only defined which consist of six exceptions/ defenses to it. With the passage of time Law interpreters felt that every defaulter takes the relief under some of the exception to strict liability and it has become a challenging task for the victim to get relief under this concept. Later on in the case of Rylands v. Fletcher [43], Judiciary led to the making of following doctrine of Absolute Liability that prevented the defendants from taking up any defense against payment of compensation. One must learn from these past mistakes, and hence, exceptions must be backed by law, and must be necessary for and proportionate to achieving the purpose of the ministry and drafters.

The Bill states that every data fiduciary shall keep a 'serving copy' of all personal and sensitive personal data in a server in India [44] but, again a power is given to Central Government of notifying certain categories of personal data as exempt from this requirement on grounds of necessity or strategic interests of the State [45]. The problem here is that, it is still not clear that what is meant by serving copy, either it could be a live, real time replication of data on a server, or it could be a backup at a specified frequency. It is necessary to provide a clear definition for serving copy as the costs, implications and implementation timelines for data fiduciaries would vary significantly. Further, it may be argued that the broad criteria for classifying data as critical needs to be specified in the law, as this is necessary for fiduciaries to prepare for the requirement of storing this data solely in India.

The Bill has defined sensitive personal data to include personal data revealing or relating to password, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe [46]. Such a broad definition of sensitive personal data (for instance, to include passwords and financial data) is not in line with international data protection laws, which have provided a much narrower definition for sensitive personal data. Therefore, foreign companies and multinational companies would face a higher compliance requirement under the data protection law in India. Such companies may find it difficult to adhere to these unique onerous compliance requirements, which would significantly affect their ease of doing business in India [47].

While Bill imposes restrictions upon data fiduciaries , it also imposes some limitations on the Rights of the data principals. Data principal may raise a complaint against data fiduciary only if a violation of the provisions of the bill has caused , or may in future cause them harm [48]. Author would again like to raise the question, why the mere violation of the rights of the data principal is not enough to raise the complaint against data fiduciary? Proving of additional harm suffered by the data principal, may place undue burden on him. The aim of DPA should be to provide maximum relief to maximum number of people, and hence there must be welcome approach at the very first instance and then after doing the preliminary inquiry, decision of the Authority as whether to admit the matter or not, should be considered final.

In India, adjudication work is done by the judicial wing of the Government. But, under this Bill an Authority is been appointed by the Central Government and is empowered with imposing penalties on data fiduciaries for violation of the provisions of the law without taking any permission or order from the Court [49]. Enforcement actions include both types of punishment, i.e., attachment or sale of movable and immovable property, and arrest and detention in prison [50]. It is also mentioned in the Bill that the DPA will enjoy all the powers of the Civil Courts prescribed to them under the Code of Civil Procedure, 1908 [51]. Hence, if the powers are enjoyed than the corelative liabilities must also be fulfilled by the authority. An Adjudicating Officer of the DPA has to determine whether the right to freedom of speech or the right to information of any other citizen could be violated by the exercise of the right to be forgotten by the data principal. "Such matters are typically interpreted by courts of law. While one of the eligibility criteria for Adjudicating Officers is knowledge and expertise in constitutional law, the Officer may be an expert in a different field, such as data protection. In such a situation, the Officer may not have the expertise to determine the constitutional question of a possible violation of freedom of speech [52]. In Authors opinion, The Bill has vested the Authority with a wide range of administrative, discretionary, quasi-legislative and quasi-judicial powers. The exercise of powers vested in the Authority under the rules adopted under the Bill, should be in a manner to avoid any concentration of multiple conflicting powers and excessive delegation, thereby defeating the purpose of the Bill. Further, the Bill does not make any provision for filing of a class action suit or a representative suit in situations where a data breach affects large number of individuals [53]."

Conclusion

Government do have recognised the problem of increasing percentage of cyber-crimes in India, the need to secure the personal privacy of an individual, and to draft a single consolidated Act on data protection in India for which they appointed the committee in order to enact a legal framework in this regime. Justice Srikrishnan committee has done a commendable work, and has also presented the first draft of the Bill in front of the Parliament within a year. In the report presented by the committee, they have also mentioned about the methodology which they have adopted to frame this bill.

Researcher would like to conclude his study by stating that, despite of the comprehensive work done by the committee there are few areas which are overlooked or drafted liberally. In India, there are prevailing laws which are dealing with prevention of cyber-crimes, Information technology, Data thefts but, the need for one single consolidated law on data protection is that there should be a well-defined procedure for collection, distribution and trade of data, key terminologies must be decided in detail, no criminal can escape from the punishment after committing the crime, to create the feeling of security among the citizens and foreign investors that their data is safe with the Government, to constitute a transparent Data Protection Authority having huge power of penalising any person for committing the offence, and to protect the vulnerable personal autonomy of an individual.

The aims mentioned above are not achieved by the committee in totality, and there is still a massive scope left for improvement in the Bill. The Bill presented before the Indian Parliament will suffice in Indian society partially, but will fail to control the increasing crime rate and will not be able to cope up with the pace of advancing technology.

References

1. W.J. Stewart and Robert Burgess, *Collins Dictionary*, 2nd ed. 2001, ISBN: 9780007102945.
2. Ministry of Communications and Information Technology, *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*, 11th April 2011, New Delhi, <https://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf>, (accessed on April 11, 2020).
3. *Ibid.*
4. Justice K.S. Puttaswamy (Retd.) v. Union of India [2019] 1 SCC 1.

5. Art. 21 of the Constitution of India stated that, "No person shall be deprived of his life or personal liberty except according to procedure established by law".
6. Supra Note 4.
7. Ministry of Electronics & Information Technology, *Office Memorandum dated 31st July, 2017*, New Delhi, <https://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf> (accessed on April 11, 2020).
8. Ministry of Electronics & Information Technology, *Public Consultation meeting dated 18th January, 2018*, Mumbai,<https://meity.gov.in/writereaddata/files/Public%20Consultation%20at%20Mumbai.pdf> (accessed on April 13, 2020).
9. *Ibid.*
10. The Personal Data Protection Bill, 2018.
11. *Ibid.*
12. Sec 3 (29) of the Personal Data Protection Bill 2018 defines the term as, "means 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, or any combination of such features, or any combination of such features with any other information".
13. Sec 3 (15) of the Personal Data Protection Bill 2018 defines the term as, "means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary".
14. Sec 3 (14) of the Personal Data Protection Bill 2018 defines the term as, "means the natural person to whom the personal data referred to in subclause (28) relates".
15. Sec 3 (13) of the Personal Data Protection Bill 2018 defines the term as, " means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data".
16. Sec 3 (11) of the Personal Data Protection Bill 2018 defines the term as, "means consent under section 12"; Sec 12 of the Bill Defines Consent as, "For the consent of the data principal to be valid, it must be free, informed, specific, clear, capable".
17. Sec 3 (16) of the Personal Data Protection Bill 2018 defines the term as, " means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal".
18. Sec 3 (21) of the Personal Data Protection Bill 2018 defines the term as, "includes bodily or mental injury; loss, distortion or theft of identity; financial loss or loss of property; loss of reputation, or humiliation; loss of employment; any discriminatory treatment; any subjection to blackmail or extortion; any denial or withdrawal of service".
19. Sec 3 (35) of the Personal Data Protection Bill 2018 defines the term as, "means personal data revealing, related to, or constituting, as may be applicable to passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or any other category of data specified under Sec. 22 of the Bill".
20. Chapter IX of the Personal Data Protection Bill, 2018.
21. Sec. 18 of the Personal Data Protection Bill, 2018.
22. Ministry of Electronics & Information Technology, *Report on Personal Data Protection Bill, 2018*, New Delhi, 2018, 55, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> (accessed on April 12, 2020).
23. Chapter II of Personal Data Protection Bill, 2018.
24. Ministry of Electronics & Information Technology, *Report on Personal Data Protection Bill 2018*, New Delhi, 2018, 74, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report .pdf>, (accessed on April 20, 2020).
25. *Ibid.*
26. PRS Legislative Research, *Draft Personal Data Protection Bill, 2018*, New Delhi, <https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018>, (accessed on April 15, 2020).
27. Sec 40(1) of Personal Data Protection Bill, 2018.
28. Sec 40(2) of Personal Data Protection Bill, 2018.
29. Sec 40(4) of Personal Data Protection Bill, 2018.
30. Sec 41 of Personal Data Protection Bill, 2018.
31. Ministry of Electronics & Information Technology, *Report on Personal Data Protection Bill 2018*, July, , New Delhi, 2018, 157, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report .pdf>, (accessed on April 18, 2020).
32. Sec 60 of Personal Data Protection Bill, 2018.
33. Sec 50 of Personal Data Protection Bill, 2018.
34. Sec 68(3) of Personal Data Protection Bill, 2018.
35. Chapter XII of Personal Data Protection Bill, 2018.
36. Chapter XI of Personal Data Protection Bill, 2018.

37. Ministry of Electronics & Information Technology, *Report on Personal Data Protection Bill*, New Delhi, 2018, 164, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report. pdf>, (accessed on April 15, 2020).
38. Ministry of Electronics & Information Technology, *Report on Personal Data Protection Bill 2018*, New Delhi, 2018, 165, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report. pdf>, (accessed on April 15, 2020).
39. Chapter XIII of Personal Data Protection Bill, 2018.
40. *Ibid.*
41. Sec. 4 of Personal Data Protection Bill, 2018.
42. Sec. 69(2) of Personal Data Protection Bill, 2018.
43. Sec. 39 (2) of Personal Data Protection Bill, 2018.
44. Sec. 12 of Personal Data Protection Bill, 2018.
45. Chapter III and IX of Personal Data Protection Bill, 2018.
46. Rylands v. Fletcher [1868] UKHL 1.
47. Sec. 40(1) of Personal Data Protection Bill, 2018.
48. Sec. 40(3) of Personal Data Protection Bill, 2018.
49. *Supra 19.*
50. Suneeth Katarki, Namita Viswanath and Ivana Chatterjee, *The Personal Data Protection Bill, 2018- Key Features and Implication*, IndusLaw Publications, 2018. <http://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications (accessed on April 15, 2020).
51. Sec. 74 of Personal Data Protection Bill, 2018.
52. Sec. 49 of Personal Data Protection Bill, 2018.
53. Sec. 60 of Personal Data Protection Bill, 2018.
54. *Ibid.*
55. PRS Legislative Research, *Draft Personal Data Protection Bill, 2018*, New Delhi, <https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018>, (accessed on April 15, 2020).
56. Suneeth Katarki, Namita Viswanath, Ivana Chatterjee. *The Personal Data Protection Bill, 2018- Key Features and Implication*, IndusLaw Publications, August 15, 2018, <http://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications (accessed on April 15, 2020).