Page 1745 - 1770 **DOI:** *https://doij.org/10.10000/IJLMH.113001*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 2

2022

Clause 35 of The Personal Data Protection Bill, 2019: Whether a Reasonable Restriction or a Withering Away of Fundamental Right to Information Privacy?

AJAY KUMAR BISHT[1] AND DR. N. S. SREENIVASULU[2]

ABSTRACT

The object of the paper is to critically examine the exception and decide thereafter whether the restriction on the right to privacy envisaged under clause 35 of the Personal Data Protection Bill, 2019 is reasonable, proportional and constitutional. It will also be examined whether the provision needs to be omitted or modified substantially or modified marginally to do justice to the subject of information privacy.

Beginning with the first available UN document on the human right namely the Universal Declaration of Human Rights, the privacy law and its limitations in the International Covenant on Civil and Political Rights will be analyzed. Thereafter, the regional human rights documents namely the European Convention of Human Rights 1950 of the Council of Europe and the Charter of Fundamental Rights of the European Union 2000 will be referred to understand the nature and scope of the human right to privacy.

The clause 35 of the PDP Bill, 2019 will then be discussed to ascertain the limitations imposed under this clause on information privacy law. The modernized Convention 108 (Convention 108+) of the Council of Europe, the General Data Protection Regulations (GDPR) of the European Union, the report of the Committee of Experts headed by Justice B.N Srikrishna, the case-law including the nine judges bench decision of the Supreme Court of India, the relevant provisions of the Constitution of India, the draft Personal Data Protection Bill of 2018 and the report of the Joint Committee of Parliament will be referred to evaluate the constitutionality of the exemption from the law proposed in the clause 35 of the Personal Data Protection Bill, 2019.

I. INTRODUCTION

We will take up the provision of clause 35 of the Personal Data Protection Bill, 2019 (the PDP Bill, 2019) which is in the nature of exception to the law of information privacy. The object of

[1] Author is Pursuing PhD from West Bengal National University of Juridical Sciences, Kolkata, India.
[2]Author is a Professor of Law at West Bengal National University of Juridical Sciences, Kolkata, India.

 [ISSN 2581-5369]

the paper is to critically examine the exception and decide thereafter whether the restriction on the right to privacy envisaged under clause 35 is reasonable, proportional and constitutional. It will also be examined whether the provision needs to be omitted or modified substantially or modified marginally to do justice to the subject of information privacy.

II. SCHEME OF THE PAPER

Beginning with the first available UN document on the human right namely the Universal Declaration of Human Rights, the privacy law and its limitations in the International Covenant on Civil and Political Rights will be analyzed. Thereafter, the regional human rights documents namely the European Convention of Human Rights 1950 of the Council of Europe and the Charter of Fundamental Rights of the European Union 2000 will be referred to understand the nature and scope of the human right to privacy.

The clause 35 of the PDP Bill, 2019 will then be discussed to ascertain the limitations imposed under this clause on information privacy law. The modernized Convention 108 (Convention 108+) of the Council of Europe, the General Data Protection Regulations (GDPR) of the European Union, the report of the Committee of Experts headed by Justice B.N Srikrishna, the case-law including the nine Judges bench decision of the Supreme Court of India, the relevant provisions of the Constitution of India, the draft Personal Data Protection Bill of 2018 and the report dated December 2021 of the Joint Committee of Parliament will be referred to evaluate the constitutionality of the exemption from the law proposed in the clause 35 of the Personal Data Protection Bill, 2019.

III. THE INSTRUMENTS AND TREATIES OF THE UNITED NATIONS

India is a founding member of the United Nations (UN). At the time of the formation of the UN in 1945, the members adopted the United Nations Charter 1945. In the Preamble to the Charter, the objects of the United Nations are stated. The objects include a reaffirmation of faith in the fundamental human rights and in the dignity of the human beings.[3]

The article 1 of the Charter includes among the purposes of the U.N, the achievement of international cooperation in promoting and encouraging respect for human rights and for fundamental freedom for all without distinction as to race, sex, language or religion.[4] The article 13 of the charter entrusts the UN General Assembly, the task of assisting in the realization of human rights and fundamental freedoms.[5] The Economic and Social Council

[3] The United Nations Charter., Preamble, The United Nations (Mar. 25, 2022)., https://www.un.org.
[4] *Id.*, art.1.
[5] *Id.*, art.13.

 [ISSN 2581-5369]

(abbreviated as ECOSOC) of the U.N, is mandated under the article 62 of the charter to make recommendations for the purpose of promoting respect for and observance of human rights and fundamental freedoms.[6] The article 55 of the charter, in general, mandates a responsibility on the U.N to promote universal respect for, and observance of human rights and fundamental freedoms.[7]

(A) The Universal Declaration of Human Rights

The United Nations General Assembly adopted the Universal Declaration of Human Rights (U.D.H.R) on 10/12/1948. [8]

The article 12 of the Declaration (UDHR) states that no one shall be subjected to arbitrary interference with his family, home or correspondence nor to attack on his honour and reputation.[9]

The researcher has quoted article 12 above because this article in the declaration became a baseline for the subsequent UN documents and treaties on privacy. Even the European Convention on Human Rights, adopted in 1950 also draws inspiration from the Universal Declaration of Human Rights of the UN. [10]

The UDHR prohibits arbitrary interference but the language permits an interference on privacy which is not arbitrary. This leaves scope for justified interference.

Thus, the UDHR itself declares that the human rights to privacy, family and correspondence is not an absolute right. However, the article 12 also provides every human being, the right to the protection against the interference on its privacy. This protection is to be provided to the person by law and the protection extends to any attack on the reputation and honour.[11] Being a member of the United Nations, India is required to take cognizance of the UDHR.

(B) The International Covenant on Civil and Political Rights

The convention called ICCPR in abbreviated form, was adopted by the United Nations in 1966 and came into force on 23/3/1976.[12] India is a signatory to the Convention. [13]

---

[6] *Id*., art. 62.
[7] *Id*., art. 55.
[8] The Universal Declaration of Human Rights (U.D.H.R), Comment before preamble, The United Nations (Apr. 13, 2022), https://www.un.org.
[9] *Id*.
[10] The European Convention on Human Rights: Convention for the Protection of Human Rights and Fundamental Freedoms. The Council of Europe (Mar. 23, 2022)., https://www.echr.coe.int.
[11] The U.D.H.R., *supra* note 8, *art*. 12.
[12] The International Covenant on Civil and Political Rights (ICCPR)., The United Nations (Mar. 23, 2022)., https://treaties.un.org.
[13] *Id*., at 266.

 [ISSN 2581-5369]

The article 17 of the ICCPR prohibits any arbitrary or unlawful interference with the privacy, family, home or correspondence of a human being.[14] The word 'unlawful' is an addition over the language of article 12 of the UDHR.

Under ICCPR too, a lawful and justified interference is permitted. Similarly lawful attacks on the honour and reputation are also permitted.[15]

Thus, the right to privacy, honour and reputation of the human being are protected to the extent that the interference on privacy and the attacks on honour and reputation should not be arbitrary or unlawful. The article 17 of the ICCPR, however provides the human beings the right to protection of the law against arbitrary or unlawful interference.[16]

(C) The UN Special Rapporteur on the right to privacy

In the year 2015, the office of the Special Rapporteur on right to privacy was created by the Human Right Council, by resolution number 28/16.[17] The office is continuing till date.

The mandates for the Special Rapporteur include reporting on the alleged violation of the provision of article 12 of the UDHR and article 17 of the ICCPR.[18] The other duties of the Special Rapporteur include the following: -

(a) Review of the policies and the legislations on the collection and processing of personal data and surveillance

(b) Assisting the member states in evolving systems to bring global surveillance under the rule of law; and

(c) Assisting the member States to ensure that national procedures and laws are in agreement with international human rights obligations.[19]

In this paper, a brief overview of some of the reports of the U.N Special Rapporteur on the right to privacy is being attempted. This will help us understand that even though the United Nations has not evolved any template of information privacy law but the units of the U.N are actively cooperating in the development and evolution of information privacy law (also called as personal data protection law).

1. Special Rapporteur's report dated 16/11/2019

[14] *Id*., at 177.
[15] *Id*.
[16] *Id*.
[17] The U.N Resolution A/HRC/RES/28/16: The right to privacy in the digital age, The United Nations (Apr. 13, 2022., https://www.daccess-ods.un.org.
[18] *Id*.
[19] *Id*.

In the report, vide Resolution No. A/HRC/40/63, the Special Rapporteur clarifies that privacy is a qualified right and not an absolute right, where an interference on privacy must be under a law and the law should also comply with the provisions, aims and the objectives of the International Covenant on Civil and Political Rights.[20] Further clarifying on the article 17 of the convention, the Special Rapporteur quoted the Human Rights Committee's comment No. 16(1988) which said that the interference provided for by law should be in accordance with the provisions, aims and objectives of the convention (ICCPR).[21] Further, any interference has to be free from 'arbitrariness; and must be reasonable in the given circumstances.[22]

The Special Rapporteur made various recommendations to the Member States to protect the personal data of the individuals. The recommendations include the following: -

(a) The Member States should ensure that all privacy-intrusive measures should be provided for by law and that the laws should be arrived at after detailed public consultation and diligent parliament scrutiny. The laws permitting infringement of privacy for the purposes of national security, defence, collective security and also for actions required for preventing, investigating and prosecuting any crime are also subject to parliamentary scrutiny;[23]

(b) The standard of 'a necessary and proportionate measures in a democratic society' is an essential parameter to ascertain whether the law enforcing agencies and the intelligence agencies are complying with the required privacy safeguards while deciding or causing any interference on privacy; [24] and

(c) Independent oversight authorities should be set up. The Member States should provide by law, adequate human and material resources to these authorities to enable them to effectively perform the task of review of privacy-intrusive events or actions.[25]

2. Report dated 24/3/2020 of the Special Rapporteur

Vide resolution number A/HRC/43/52, the Special Rapporteur recommended to the Member States to adopt the technologies including 'encryption', 'pseudonymization' and 'anonymiza-

[20] Resolution No. A/HRC/40/63 dated 16/10/2019, The United Nations (Mar. 26, 2022)., https://www.ohchr.org.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

 [ISSN 2581-5369]

tion' to protect the privacy rights of the individuals in digital communication.[26]

The other recommendations made by the Special Rapporteur include the following: -

(a) The amendment of the existing laws on surveillance, cyber-crime and cyber-terrorism be made to bring these laws into conformity with the international human rights laws and instruments related to the rights of privacy; freedom of opinion and expression; and peaceful assembly and association;[27]

(b) Safeguards by law should be provided against the non-consensual, predatory, commercial surveillance that results in aggregation, profiling and marketing through the use of big data technologies including mobile geo-fencing and geospatial location markers.[28]

The flavour of the contribution to the right to privacy made by the Special Rapporteur becomes clearer if we refer to a few more reports.

3. Report dated 23/7/2021; Resolution No. A/76/220 on data protection during COVID-19

The impact of the measures taken by the Governments and the non-Government organizations during covid-19 was studied in detail by the Special Rapporteur. In legal terms, a very significant comment was made by the Special Rapporteur that the people around the world had surrendered various aspects of their privacy and freedoms in order to fight the corona virus.[29]

The Special Rapporteur reported that the measures taken by the countries had adversely impacted the rights of freedom of expression (57 countries); freedom of assembly (147 countries) and the right to privacy (70 countries).[30]

It reported that actions of the Government and the technology companies have raised concerns about the necessity and proportionality of the personal data collected during COVID-19 and the security as well as the secondary use of the data.[31] Considering the infringement of privacy faced during COVID-19, the Special Rapporteur recommended to the Member States to protect the personal data even during the pandemic. The recommendations included the following:

[26] Resolution No.A/HRC/43/52, dated 24/3/2020, The United Nations (Mar. 26, 2022)., https://www.ohchr.org.
[27] *Id.*
[28] *Id.*
[29] Resolution No. A/76/220, dated 23/7/2021, The United Nations (Mar. 26, 2022)., https://www.ohchr.org.
[30] *Id.*
[31] *Id.*

(a) The 'privacy by design' and 'privacy by default' may be built in the system which can facilitate an overarching privacy right assessment for public health activities.[32]

(b) At the earliest response to any epidemic or pandemic, the aspect of privacy should be flagged.[33]

(c) Clear and comprehensive privacy protection provisions may be incorporated in the data protection law of nation or the region.[34]

(d) The law on the data protection should itself contain clear and detailed provisions and the reliance on the delegated legislation for the data protection should be minimized.[35]

(e) Even during medical emergencies and pandemic, the data collection and processing should follow data minimization and purpose limitation principles so that the injury or damage caused to the individual due to personal data breach or cyber incidents is minimized.[36]

(f) 'Sunset clause' and independent 'audit of closure' should be compulsorily included in the epidemic data systems.[37]

(g) An independent data protection authority should regularly supervise the data surveillance system even during the epidemic.[38]

(h) The health emergency powers and relaxation of the Members States need to be assessed to examine the elements of 'necessity' and 'proportionality'.[39]

4. Report dated 13/1/2022.

The resolution number A/HRC/49/55 dated 13/1/2022 is in respect of the report of the Special Rapporteur on the data protection laws and technology in Ibero-American nation States. The contents of the report are however relevant to our study on the aspect of data protection in general. The Special Rapporteur suggested that the Ibero-American data protection system provides a framework for working collaboratively towards globally accepted data protection

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*

 [ISSN 2581-5369]

principles.[40] The Special Rapporteur stated that the right to privacy is established as a fundamental human right in the Constitutions of most of the Ibero-American States.[41]

(D) Evolution of a globally agreed template on information privacy law.

In the past, the United Nations General Assembly has adopted modern draft legislations. The Model law on Electronic Commerce was one such draft law adopted by the General Assembly by resolution No. A/RES/51/162 dated 30/01/1997. This draft law was adopted with modifications by the Indian Legislature and was enacted into the Information Technology Act, 2000.

After reading the report dated 13th January 2022 of the Special Rapporteur, it seems possible that the United Nations General Assembly may evolve a draft of Data Protection Law in the near future.

The ICCPR has the force of law in India because India is a signatory to it and the articles 51(c) and 253 of the Constitution of India empower the Union Legislature to make enactment related to the international treaties and agreement. So, India will find it convenient to adopt with necessary modification a law which is suggested by the United Nations.

After examining the provisions of the instruments of the United Nations, the researcher purposes an overview of the European regional instruments.

IV. THE INSTRUMENT AND TREATIES OF THE EUROPEAN REGION

The countries of Europe were the front runners in entering into regional treaties. The Council of Europe was formed in 1949 and the European Union was formed in 1993.

Going in the chronological order of the resolutions, first we study the European Convention on Human Rights, 1950 of the Council of Europe.

(A) The European Convention on Human Rights.

The European Convention on Human Rights (abbreviated as ECHR) is also called the Convention for the Protection of Human Rights and Fundamental Freedoms and was adopted by the Council of Europe on 4/11/1950.[42] The Convention is inspired by the Universal Declaration of Human Rights, 1948 of the United Nations.[43]

[40] Resolution no. A/HRC/49/55, dated 13/1/2022, The United Nations (Mar. 26, 2022)., https://www.ohchr.org.
[41] *Id*.
[42] The European Convention on Human Rights., *supra* note 10, at 1., https://www.ohchr.coe.in.
[43] *Id*.

The article 8.1 of the Convention guarantees to every individual, the right to privacy, family life, home and correspondence.[44] The article 8.1 is positively worded and gives a right to the individual whereas, the article 12(1) of the UDHR was negatively worded and prohibited the arbitrary interference with privacy.

However, article 8.2 of the ECHR prohibits any interference by the State in the exercise of the right by the individual.[45] However, the right in the ECHR like the right stated in the UDHR, is not an absolute right. The article 8.2 permits interference with the right to privacy if the interference is by law and is necessary in a democratic society in the interest of national security, public safety, the protection of the rights of others and the freedom of others.[46]

By the time of adoption of ECHR (i.e., in 1950, the ICCPR had not come into being, as it was adopted by the United Nations in 1966.

1. Derogation of the rights in time of emergency.

The right under article 8.1 can be restricted in the event of public emergencies which could threaten the life of the nation.[47] The public emergencies include war. A condition is however laid down under article 15.1 that the measure restricting or relaxing the right of the individual should be necessary under the exigencies of the circumstances and should not be in violation of any other obligation under the Convention.[48]

While the right to privacy is not absolute, the article 15.3 provides that a derogation of the right to privacy resorted to by the State in case of public emergency needs to be notified to the Secretary General of the Council of Europe.

2. The Convention 108.

The Council of Europe adopted on 28/1/1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ('The Convention 108' in short).[49] The Convention is the first ever international instrument available on the protection of personal data (also called information privacy). The Convention was, however, modified in the year 2018 after the European Union had evolved the G,D.P.R in 2016. The modified version is called Modernized Convention 108 (or in short 'Convention 108+'). We shall be discussing in detail,

[44] *Id.*, at 1.
[45] *Id.*
[46] *Id.*
[47] *Id.*, at 12.
[48] *Id.*
[49] The Convention 108., The Council of Europe (Mar. 26, 2022)., https://www.m.coe.in.

the provisions of Convention 108+ in the later sections while analyzing the provision of the Personal Data Protection Bill, 2019.

(C) The Charter of Fundamental Rights of the European Union.

After the establishment of the European Union in the year 1993, the Union adopted the Charter of Fundamental Rights of the European Union (CFREU) on 7/12/2000. The Charter came at the time when data protection had already been incorporated in Convention (Convention 108) of the Council of Europe.

The article 7 of the Charter is worded similar to the article 8.1 of the European Convention on the Human Rights. The article 7 provides everyone in its jurisdiction the right to expect respect for his privacy, family life, home and correspondence.[50] The article 8 of the Charter contains provision specific to data protection. The article 8.1 of the charter grants everyone the right to protect his/her personal data.[51] The article 8.1 puts an obligation on the processors (and controllers) of the personal data to process the data on the basis of consent of the individual where the consent is given for specific purpose.[52]

However, the article 8.2 permits non-consensual processing of the personal data of the individual for some legitimate purpose laid down by law.[53] The article 8.2, further, provides the individual with the right to access personal data and also the right of rectification of its personal data.[54]

The article 8.3 of the Charter provides for an independent authority to monitor the compliance of the article 8.1 and 8.2.[55] Thus, the article 8 of the Charter presents a broad guidance on the protection of personal data. It acknowledges that the right is not absolute and permits the processing if it is laid down by law for legitimate reasons.

1. Conditions under which limitation on data protection can be enforced.

The article 53.1 of the Charter provides that any limitation on the exercise of the rights under the charter must be provided for by law and must respect the spirit of the rights and freedom

[50] The Charter of Fundamental Rights of the European Union, article 7., Official Journal of European Union, 26/10/2012., (Mar. 26, 2022)., www.eur-lex.europa.eu.
[51] *Id*., article 8.1.
[52] *Id*., article 8.2.
[53] *Id*.
[54] *Id*.
[55] *Id*.

of individuals.[56] In addition to this, the article 53.1 requires that the law limiting the right should pass the test of 'necessity' and 'proportionality'.[57]

(D) The Directive 95/46/EC of the European Union.

The European Union had adopted the Directive Number 95/46/EC on 24/10/1995.[58] The Directive has, however, been repealed in 2016 and replaced by the regulation (EU) 2016/679, in short called the General Data Protection Regulations (GDPR).[59] The provisions of the GDPR would be referred to in the later sections while examining the provisions of the Personal Data Protection Bill, 2019.

After this survey of the European regional treaties and instruments on privacy, we have been enriched with a good amount of persuasive authorities and also by analytical tools which are similar for data protection and data processing operations all over the world.

After this survey of international instruments and treaties, now we examine the provisions of the clause 35 the Personal Data Protection Bill, 2019. The provision related to exemption from the information privacy law is being examined with the object of finding whether the exemption is constitutional or not.

V. CLAUSE 35 OF THE PDP BILL, 2019: EXEMPTION OF ANY GOVERNMENT AGENCY FROM ALL OR ANY PROVISION

The clause 35 is among the most controversial if not the most controversial clause of the Personal Data Protection Bill, 2019. The clause empowers the Central Government to exempt any Government agency from all or any of the provisions of the Act.[60]

Justice B.N Srikrishna had headed the Committee of Experts appointed by the Government in July 2017 to study the issues relating to data protection in India and to suggest a draft of Data Protection Bill.[61] The Committee of Experts had proposed a draft Bill called the Personal Data Protection Bill, 2018(the PDP Bill, 2018). The PDP Bill, 2018 did not have any provision of granting complete exemption to any agency (whether Government or non-Government) from all the provisions of the Act.

---

[56] *Id.*
[57] *Id.*
[58] The Directive 95/46/EC of the European Parliament and of the Council of 24th October, 1995 on the protection of individuals with regard to processing of personal data and the free movement of such data., The Council of Europe (Mar. 26, 2022)., https://eur-lex.europa.in.
[59] Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016 (General Data Protection Regulation)., The Council of Europe (Mar. 5, 2022)., https://eur-lex.europa.en.
[60] The Personal data Protection Bill, 2019., p. 19., The Parliament of India (Mar. 5, 2022)., https://164.100.47.4.
[61] Office memorandum No. 3(6)/2017-CLES dated 31/7/20 To the Ministry of Electronics and Information Technology, Govt. of India (Mar. 26, 2022)., https://www.meity.gov.in.

Referring to the clause 35 of the PDP Bill, 2019, Justice B.N Srikrishna feared that the 2019 Bill would lead to an Orwellian State.[62] A scholar has also commented that the clause 35 of the PDP Bill, 2019 enhances the powers of the Government to conduct surveillance.[63] A cyber security expert has on the other hand, argued that the PDP Bill, 2019 can actually reduce the surveillance powers of the State and that the Bill balances the citizen's right to privacy with internet security.[64] Another scholar opined referring to clause 35 of the Bill that the possibility of harassment, blackmail and coercion rise with the rise in the concentration of the State power.[65] We now examine the contents of the provision to arrive at a fair assessment of the proposed law.

(A) The satisfaction of the State Government: necessary or expedient

The clause begins with the words 'where the Central Government is satisfied that it is 'necessary or expedient'. The satisfaction has to be of the Central Government i.e. the Union Government. The word 'necessary' means 'essential' and the word expedient means 'something suitable for achieving an object in a given situation'.

The ingredients of the first part of the first sentence of the clause mean that the Central Government will resort to this provision in order to achieve some particular purpose or when the Central Government finds it essential to invoke.

To understand the important of these words we may refer to some provisions of the Constitution of India where these words are used.

1. Article 239 AB: Failure of Constitutional Machinery in NCT of Delhi.

The article 239 AB of the Constitution of India empowers the President of India to suspend the operation of any provision of article 239AA when the President is satisfied that it is necessary or expedient to do so.[66] The article 239 AB is akin to article 356 which provides for the Union Parliament and Government the power to assume the legislative and executive powers of the State Legislature and Government.

2. Article 249(1): Parliament to legislate on State List subject.

[62] Megha Mandavia: "Personal Data Protection Bill can turn India into 'Orwellian State' - Justice B.N Srikrishna", The Economic Times, dated 31/1/2020, (Mar. 26, 2022)., https://economictimes.indiatimes.com.
[63] Kazim Rizvi: "Personal Data Protection Bill, 2019 and Surveillance: Balancing Security and Privacy" date not available, (Mar. 26, 2022)., https://inc42.com.
[64] Omkar Khandekar : " Data Protection Bill can reduce the state's surveillance powers", article dated 15/8/2020, (Mar. 26, 2022)., https://lifestyle.livemint.com.
[65] Aditi Agarwal : " NAMA: Issues Around Surveillance in the Personal Data Protection Bill, 2019" article dated 29/1/2020, (Mar. 26, 2022)., https://www.medianama.com.
[66] P.M BAKSHI: The Constitution of India., (Lexis Nexis, 2020).

 [ISSN 2581-5369]

The article 249(1) empowers the Council of States (i.e. the Rajya Sabha), if by a resolution supported by at least two third of the members present and voting, it finds it necessary or expedient it may entrust the law-making power on any matter of the State list to the Parliament.[67]

3. Article 312(1): Creation of All India service.

Under the article 312(1), the Council of States, by a resolution supported by at least two third of the members present and voting can approve the creation of an all-India Service, if it finds such creation necessary or expedient.[68]

Thus, it is seen that the words 'necessary or expedient' appear in this form in the Constitution when some extraordinary power is being considered to be invoked to handle an extraordinary situation. It implies that the invokation of such power would be rare and uncommon.

(B) Grounds for invoking extraordinary powers

To examine the grounds on which it will be necessary or expedient to invoke the provision, we turn to the next part of the clause 35 which is sub-clause (1).

The terms 'in the interest of sovereignty and integrity of India', 'the security of State' and 'public order' mentioned in sub-clause (1) are inter-related and each one of these grounds relates to the security of the nation. The ground 'relation with foreign States' relates to the diplomatic relations of the nation and generally is considered a matter of foreign policy on which the Central Government is expected to take a decision in national interest.

1. Article 4 of the ICCPR: Derogation from the human right to privacy

The article 4 of the United National document, namely the International Covenant on the Civil and Political Rights permits the Member States to derogate from the human rights (including the right to privacy) in the event of any public emergency.[69] The researcher finds that all the four grounds provided in this part of the clause 35 qualify to be the ground for a public emergency, depending on the degree or magnitude of the perceived threat to the security of the state or the public order. So, the public emergency would need to be examined by the State on case-by-case basis before an opinion to invoke the provision of restriction of rights of the individual is formed.

[67] *Id.*
[68] *Id.*, at 367.
[69] The ICCPR., *supra* note 12, at 174.

2. Article 11 of Convention 108+: Derogation from the right to information privacy for national security, etc.

The article 11.1.a of the Modernized Convention (Convention 108+) of the Council of Europe provides for exceptions to the right of information privacy if made by law in the interest of national security, defence of the nation, public safety and other essential objectives of public interest.[70]

3. Article 23 of the GDPR: Restrictions on the right to information privacy for national security etc.

The articles 23.1.a, b and c of the GDPR of the European Union permit the restriction of the right to information privacy by a law made on the grounds of national security, defence of the nation and public security.[71]

4. Article 19(2) of the Constitution of India: Reasonable Restriction

Article 19(2) of the Constitution of India permit the restriction made by law on the fundamental right to 'freedom of speech and expression' on the grounds including the sovereignty and integrity of India, the security of the State, friendly relations with the foreign States and public order.[72]

5. Section 5 of the Indian Telegraph Act, 1885: Restriction on the right to information privacy.

The section 5(2) of the Indian Telegraph Act, 1885 permits the State to impose restrictions on transmission or receipt of information on the grounds including sovereignty and integrity of India, the security of the State, friendly relations with the foreign states and public order subject to the condition that the State considers such a restriction necessary or expedient.[73]

6. Section 69 of the IT Act, 2000: Limitation on the right to information privacy.

The section 69 of the IT Act, 2000 permits the Central and the State Governments to intercept, monitor or decrypt any information if the said Government finds it necessary or expedient on

[70] Convention 108+: Convention for the protection of individuals with regard to the processing of personal data., at 9., The Council of Europe (Mar. 3, 20122) https://www.europarl.europa.en.
[71] 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 free movement of such data., at L119/46-47., The Council of Europe (Mar. 5, 2022)., www.eur-lex.europa.eu.
[72] P.M BAKSHI., *supra* note 66, at 57.
[73] The Indian Telegraph Act, 1885., No. 13 of India (Mar. 27, 2022)., https://www.indiacode.nic.in.

the grounds including sovereignty and integrity of India, security of the State, friendly relations with the foreign States or public order.[74]

(C) The judgment in Puttaswamy (2017): Privacy a fundamental right.

The unanimous decision of the nine- Judge bench, dated 24/8/2017 declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as part of the freedoms guaranteed by part III of the Constitution.[75]

The Apex Court found privacy as residing inside the articles including article 21. So, a discussion on privacy without taking into account the right to life and personal liberty would be an incomplete exercise. The researcher, therefore, now examines the limitations that can be imposed on the right conferred by article 21 of the Constitution of India.

(D) Rights in article 21: Whether derogable under Law and case-law?

The article 21 of the Constitution of India permits the restrictions on the right to life and personal liberty through a procedure establish by law.[76]

However, the article 359 of the Constitution which permits the restriction on rights during an emergency accords utmost priority to the rights conferred in article 20 and 21 by not permitting the derogations of these rights even when the emergency has been enforced in the whole or any part of the country.[77] Thus article 359 implies a non-derogable status to the rights conferred under article 21.

1. Smt. Selvi v State of Karnataka (2010): Article 21 non-derogable.

In its order dated 5/5/2010, the Apex Court affirmed in para 216 that the rights guaranteed in the article 20 and 21 of the Constitution of India have been given a non-derogable status and that these rights are available to all persons whether citizen or not.[78] The Court, in the case had observed that the administration of the evidentiary tests like the polygraph and narco-analysis violates the standard of 'substantive due process' which is the pre-condition for placing any restriction on personal liberty.[79]

2. PUCL v Union of India (1996): Article 21 derogable?

[74] The Information Technology Act, 2000., No. 26, Acts of Parliament, 2000 (India) Mar. 3, 2022)., https://www.indiacode.nic.in.
[75] Justice K.S Puttaswamy (Retd.) v Union of India, WP(C) No. 494 of 2012, order of the court, 24/8/2017, at 3 (Mar. 27, 2022)., https://www.main.sci.gov.in.
[76] P.M BAKSHI., *supra* note 64, at 74.
[77] *Id*., at 404.
[78] Smt. Selvi v State of Karnataka, Criminal Appeal no. 1267 of 2004, order dated 5/5/2010, (Mar. 27, 2022)., https://indiankanoon.org.
[79] *Id*., para 222.

Vide the order dated 18/12/1996, the Apex Court in para 18 held that the right to privacy is part of the right to 'life' and 'personal liberty' guaranteed under article 21 of the Constitution.[80] Further, in para 19, the Court declared that telephone tapping would violate privacy and infringe article 21 of the Constitution when the tapping is not permitted under the procedure established by law.[81] In para 166, the court recommended that the telephones can be tapped in the interest of the national security, public order, investigation of crimes and similar objectives under orders made in writing by the Minister or an officer who is delegated the power.[82]

The court thus, did not find the rights conferred under article 21 of the Constitution non-derogable. While upholding the provision of section 5 of the Telegraph Act, 1885, the court issued guidelines to frame rules as per the corresponding rule making provision i.e. section 7 of the Telegraph Act, 1885.

3. Puttaswami(2017): Whether article 21 derogable?

The lead judgment dated 24/8/2017 in K.S. Puttaswamy v. Union of India held in para 165 of the judgment that a law can be challenged on the ground of violation of article 21 of the constitution, unless the procedure established by the law is fair, just and reasonable.[83]

Thus the rights conferred under article 21 (including the right to privacy) are not absolute and are derogable subject to a fair, just and reasonable procedure established by law.

(E) Reasoned order in writing : Electronic form?

The next part of the clause 35 after sub-clause (ii) permits the Central Government to exempt, by a reasoned order in writing any agency of the Government from all or any of the provisions of the Act, for processing of personal data.[84]

It is fair that the order under the clause 35 has to be in writing and the Central Government has to cite the circumstances necessitating the order. A reasoned order is a requirement of administrative law and is an effective check on the arbitrary exercise of authority.

It is noteworthy to add that in this computerised age, writing could mean electronic recording also. The section 4 of the IT Act, 2000 permits the rendering in 'electronic form', any information or matter that the law requires in written form.[85]

[80] People's Union of Civil Liberties v Union of India, order dated 18/12/1996., (Mar. 27, 2022)., https://indiakanoon.org.
[81] *Id*.
[82] *Id*.
[83] Justice K.S. Puttaswamy v. Union of India., supra note 75, four Judges order dated 24/8/2017., at 240.
[84] The PDP Bill, 2019., *supra* note 60, at 19.
[85] The IT Act, 2000., *supra* note 74, at 9.

This aspect is relevant because, the orders in favour of an agency may be issued and acted upon in electronic form within a short span of time while the stakeholders at large, might not be aware of the issuance of such order which is available only in electronic form. Thus the technological literacy (or technical literacy) is a requirement for every person in this digital age. The researcher fears that a large number of helpless individuals might not be able to decipher or comprehend the swift manner in which the Government might issue orders in electronic form.

(F) Exemption from all or any of the provisions

The exemption from all the provisions of the Act would mean that the Act does not apply to the agency that has been ordered to be exempted under clause 35 of the PDP Bill, 2019. The critics of the clause 35 have gone to the extent of commenting that such a provision could unleash a regime of surveillance. Justice B.N. Srikrishna who headed the Committee of Experts have expressed suspicion that the provision of clause 35 could turn India into an Orwellian state.[86] In a democratic state, the governance needs to be fair and it ought to appear fair too. Even if the fears of people in a democracy are unfounded, the researcher feels, the fears need to be addressed diligently.

'Orwellian State' is a metaphor used for a State characterised by perpetual surveillance. It is based on the fiction novel titled 'Nineteen Eighty Four' authored by George Orwell. Originally written in 1949, the book offers a nightmarish vision of a totalitarian state with a gloomy future for the inhabitants.[87]

The present times have witnessed the exposes of Edward Snowden. Since the year 2013, Snowden has been disclosing how the personal data collected and processed in the network of the corporate bodies engaged in the information and communication sector is being used by the State agencies of the United States to conduct surveillance on the helpless individuals.[88]

While exemption from few particular provisions of the law might not create so much fear, an absolute exemption does create fears when the Government of the day is granted the power to exempt an agency from all the provisions of any law, particularly any law protecting the right of the individuals.

(G) Any corresponding provision in the draft Bill of 2018?

[86] Megna Mandavia., *supra* note 82.
[87] GEORGE ORWELL : NINETEEN EIGHT FOUR, 1949., (Mar. 27, 2022)., https://www.goodreads.com.
[88] Ewen Macaskill and Gabriel Dance: 'NSA files : decoded'., The Guardian, Nov. 1, 2013 (Apr. 13, 2022)., www.theguardian.com

 [ISSN 2581-5369]

The draft Personal Data Protection Bill, 2018 prepared by the Committee of Experts headed by Justice B.N. Srikrishna did not have any provision to exempt any agency (whether Government or non-Government) from all the provisions of the Act. The draft Bill, however, had provided for limited exemption under clause 42.

1. Clause 42 of the PDP Bill, 2018.

The clause 42 of the 2018 Bill had provided for exemption of processing of personal data for the purpose of national security. The exemption was contemplated for a majority of the provisions of the Act and that the exemption was to be authorised by a law.[89] The exemptions permitted related to the provisions of the law dealing with data protection obligations, grounds for processing personal data, grounds for processing sensitive personal data, processing of sensitive data of children, rights of the data principal, transparency and accountability obligations and the transfer of personal data outside India.[90]

2. Opinion of the Committee of Experts on exemption for national security.

The Committee of Experts which drafted the P.D.P. Bill, 2018 was cautious of the potential misuse of the provision of exemption in the ostensible name of national security. Moreover, the Committee favoured only partial exemption from the data protection law for the purpose of security of the State.[91] The Committee had noted that in the United States, the United Kingdom, Germany and South Africa, the provision of external oversight over the surveillance agencies was built in the law, but in India such an oversight mechanism did not exist.[92]

The Committee argued that the judgment dated 24/8/2017 of the Supreme Court of India in K.S. Puttaswamy v. Union of India had laid down that any exception to the right to privacy must satisfy three conditions (also called 'triple test'). The first test is that the exception should be provided by law, the second test is that the exception must be a necessary and proportionate measure and the third test is that the exception must be made in fulfilment of a legitimate State interest.[93]

The Committee thus, did not include a provision of complete or partial exemption in favour of any agency by an executive action. Even partial exemption, in the opinion of the Committee need to be provided by a law. So the draft PDP Bill, 2018 did not have any provision similar

[89] The Personal Data Protection Bill, 2018., at 25, (Mar. 27, 2022)., www.meity.gov.in/writereaddata/files.
[90] *Id*.
[91] A FREE AND FAIR DIGITAL ECONOMY : PROTECTING PRIVACY, EMPOWERING INDIANS, 2018., at 123 (Mar. 27, 2022)., www.meity.gov.in/writereaddata/files.
[92] *Id*., at 127.
[93] *Id*.

 [ISSN 2581-5369]

to the clause 35 of the PDP Bill, 2019. That explains the anxiety of Justice B.N. Srikrishna, who had headed the Committee.

(H) Procedure, Safeguards and oversight mechanism to be followed by the exempted agency

The clause 35 further provides that the procedures, safeguards and oversight mechanism over the functioning of the exempted agency will be provided through subordinate legislation by rules.[94]

The Rule 419A of the Indian Telegraph Rules, 1951 lay down the procedure, the safeguards and the oversight mechanism under the Indian Telegraph Act.[95] The rules are being implemented in India and any regulatory crisis or over regulation under these rules is not reported.

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 framed under the section 69 of the IT Act, 2000 provide the procedure, safeguards and the oversight mechanism under the IT Act.[96] The rule 2(q) of these rules provide that the Review Committee for monitoring the interception would be the same as the Review Committee constituted under the Indian Telegraph Rules, 1951.[97]

In the context of India, the provision of prescription of procedure, safeguards and the oversight mechanism through rules seems to be a workable and an effective arrangement.

(I) The views of the Joint Committee of Parliament on clause 35.

The Joint Committee of Parliament (JPC) examined the clause 35 with the perspectives of two competing interests namely 'national security' and privacy. The Committee (JPC) opined that security of the nation is more important than liberty (including privacy) because only a secure nation can provide the conditions conducive for the exercise of the right to privacy.[98]

The Committee reasoned that the judgment of 2017 in **Puttaswamy** had permitted the restricting of the right to privacy by a law if the action is for a legitimate aim and the restriction on the right to privacy is proportionate and that the potential abuse of the restriction is prevented

[94] The PDP Bill, 2019., *supra* note 60, at 19.
[95] Notification G.S.R. 193(E) dated 01/3/2007, Ministry of Communication and Information Technology, Government of India (Mar. 27, 2022)., https://www.dot.gov.in.
[96] Notification G.S.R. 780(E) dated 27/10/2009. Ministry of Electronics and Information Technology, Government of India (Mar. 27, 2022)., https://www.meity.gov.in.
[97] *Id*.
[98] Report of the Joint Committee on the Personal Data Protection Bill, 2019., at 115., Lok Sabha Secretariat, New Delhi, December, 2021 (Mar. 27, 2022)., https://www.internetfreedom.in.

 [ISSN 2581-5369]

by adequate safeguards.[99] The Committee referred to the restrictions on the right to privacy permitted under article 23 of the GDPR for national security, defence and public safety.[100]

The Committee was of the view that 'national sovereignty and integrity', 'security of the State', 'friendly relations with foreign states' and 'maintenance of public order' are priority concerns for a nation in the existing geo-political circumstances.[101] The Committee noted that the provisions of clause 35 of the PDP Bill have precedents in the reasonable restrictions permitted under article 19(2) of the Constitution.[102] The Committee argued that the provisions of clause 35 have a basis in the Puttaswamy judgment and have precedents in the Information Technology Act, 2000 and the Indian Telegraph Act, 1885.[103]

The Committee felt that the State is within its power to exempt its agencies from the application of the Act, but the power of exemption should be used only under exceptional circumstances.[104] The Committee suggested following two changes to the provisions of clause 35:-

a) addition of the words 'Notwithstanding anything contained in any law for the time being force' in the opening sentence of the clause 35; and

b) addition of a new sub-clause to the explanation appended to clause 35 to make a sub-clause (iii) to the explanation as '(iii) the expression "such procedure" refers to just, fair, reasonable and proportionate procedure.'[105]

(J) Precedence of restrictions comparable to clause 35.

The contents of the provision of clause 35 have precedents in the other legislations of the electronic communication sector namely the section 69 of the IT Act, 2000[106] and the section 5(2) of the Indian Telegraph Act, 1885.[107]

The grounds for restricting the right to privacy under clause 35 are also included in the grounds for imposing reasonable restrictions on the right to freedom of speech and expression under article 19(2) of the Constitution of India.[108] The grounds of imposing reasonable restrictions under article 19(2), 19(3), 19(4), 19(5) and 19(6) are however, all different.[109] Thus for

[99] *Id.*
[100] *Id.*, at 117.
[101] *Id.*, at 119.
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*, at 120.
[106] The I.T. Act, 2000., *supra* note 74., at 26.
[107] The Indian Telegraph Act, 1885., *supra* note 73., at 5.
[108] P.M. BAKSHI., *supra* note 66, at 57.
[109] *Id.*, at 57-58.

different kinds of rights, the grounds for restrictions are different or at least the grounds can be different.

Further, the climate of opinion about right to privacy has undergone a change after the disclosures of Edward Snowden from 2013 onwards. This climate of opinion has further undergone changes in favour of privacy after the nine Judges unanimous judgment of 2017 in K.S. Puttaswamy v. Union of India. The restrictions on privacy which appeared reasonable a decade back, would today seem unreasonable.

The JPC's suggestion of adding the 'non obstante' clause in the beginning of clause 35 would strengthen the efficacy of the provision of clause 35.

The addition of sub-clause (iii) to the explanation below clause 35 would sensitize the executive wing and the government agency which has been granted exemption from the Act, to follow fair, just, reasonable and proportionate procedure.

VI. CONCLUSION AND SUGGESTIONS

The researcher thus concludes that the provision of exemption contemplated in the clause 35 of the Personal Data Protection Bill, 2019 (the P.D.P. Bill, 2019) does not cause the withering away of the fundamental right of the individual to information privacy.

The provision is a restriction on the right to information privacy. However, the provision appears unreasonable due to the scope extending upto absolute exemption. The provision of clause 35, therefore, needs to reviewed and reworded with the corresponding changes as discussed below.

(A) Provision of only partial exemption under clause 35

The researcher suggests that the clause 35 may provide only for partial exemption, i.e. the government agency may be exempted from the applicability of certain sections as is provided for other exemptions under the clause 36 of the PDP Bill, 2019. It may not be appropriate to include a provision of complete exemption from the law in the middle of the provisions of the law. Such a complete exemption would be incongruous with the flow of the provisions.

(B) Provision of 'Complete Exemption' to be made in the applicability portion of the Act.

A sub-clause (C) below the sub-clause (B) in clause 2 of the P.D.P. Bill, 2019 may be inserted as '(C)' shall not apply to the agencies or organizations of the Government listed in the schedule appended to the Act.

 [ISSN 2581-5369]

Such a provision of exemption of listed documents exist in the IT Act, 2000 where section clause (4) of section 1 provides that the Act shall not apply to the documents or transaction specified in the First Schedule.[110] The First Schedule to the IT Act, 2000, has presently, listed five documents including a negotiable instrument (other than a cheque) and a power of attorney.[111]

The spelling out of the provision of inapplicability of the law in the opening parts of the law would fulfil the requirement that the exemption to the law needs to be provided by law.

(C) The Central Government to be competent to amend the Schedule

The subject matter of the law relates to the entry 31 of the Union List and so the Central Government alone is competent to legislate on the subject.

A proviso to the sub-clause (C) of the clause 2 may be added as:

'Provided that the Central Government may, by notification in the Official Gazette, amend the schedule by way of addition or deletion of entries thereto.'

(D) Amendment of the Schedule to be placed in Parliament

A second proviso to the sub-clause (C) of clause may be added as 'Provided further that every notification issued under the clause (C) shall be laid before each House of Parliament.'

Such a proviso will provide the parliamentary oversight which is a safeguard against the arbitrary exercise of power by the Executive wing.

(E) Effective promotion of technological literacy

While the provisions of restriction on the fundamental right of liberty on similar lines exist in Article 19(2) of the Constitution the section 5(2) of the Indian Telegraph Act, 1885 and the section 69 of the Information Technology Act, 2000 but the scholarly writings in India have largely assailed the provision of clause 35 of the PDP Bill, 2019. This may be due to ignorance of these existing laws.

The fear of Orwellian surveillance also result from the lack of technological literacy related to information technology.

The State including the Union and State Government may, in right earnest provide the material, academic and human resources to enhance the technological-literacy (also called 'technical literacy') among the people.

[110] The I.T. Act, 2000., *supra* note 74., at 5.
[111] *Id*., at 36.

 [ISSN 2581-5369]

A recommendation to strengthen technical literacy has been repeatedly emphasized by Edward Snowden (the ex-spy who exposed the unfair surveillance done by the Government agencies of the United States) also.

(F) An Advisory Committee to advise the Data Protection Authority to promote technical literacy

The provision of an Advisory Committee may be made in the P.D.P. Bill, 2019. Such a Committee representing the experts of the law, information technology, cyber law, academia, business and public service can provide effective recommendation to Data Protection Authority (DPA) for promoting technical literacy.

Such provisions of Advisory Committee exists in various Central legislations including the Electricity Act, 2003 (section 80 and 87), the Insurance Regulatory and Development Authority Act, 1999 (section 25) and the Information Technology Act, 2000 (section 88). Advice from such professionals and expert would provide a two way communication between the State and the people. This would be in a true spirit of democracy.

*****

 [ISSN 2581-5369]

VII. REFERENCES

(A) INDIAN LAWS AND LEGISLATIVE PROPOSALS

1. The Constitution of India.
2. The Indian Telegraph Act, 1885.
3. The Information Technology Act, 2000.
4. The Personal Data Protection Bill, 2019.
5. The Personal Data Protection Bill, 2018.
6. Rule 419 A, The Indian Telegraph Rules, 1951.
7. The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

(B) THE CASE-LAW OF THE SUPREME COURT OF INDIA

1. Justice K.S Puttaswamy v Union of India ,WP(C) 494 of 2012, order dated 24/8/2017
2. Smt. Selvi v State of Karnataka, Cr Appeal No. 1267 of 2007, order dated 5/5/2010.
3. People's Union of Civil Liberties v Union of India, order dated 18/12/1996.

(C) REPORTS OF THE PARLIAMENTARY/ OTHER COMMITTIES.

1. The Report of the Joint Committee on the Personal Data Protection Bill, 2019, Lok Sabha Secretariat, December 2021.
2. 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians'. Report dated 2018 of the Committee of Experts (headed by Justice B.N Srikrishna) appointed by the Government of India to suggest a draft of data protection law.

(D) THE DOCUMENTS, INSTRUMENTS AND REPORTS OF THE UNITED NATIONS ORGANIZATION.

1. The United Nations Charter, 1945.
2. The Universal Declaration of Human Rights, 1948.
3. The International Covenant on the Civil and Political Rights, 1966.
4. The U.N Resolution A/HRC/RES/28/16 dated 01/04/2015: The right to privacy in the digital age.

 [ISSN 2581-5369]

5. The U.N Resolution A/HRC/40/63 dated 16/10/2019: Report of Special Rapporteur on right to privacy.
6. The U.N Resolution A/HRC/43/52 dated 24/3/2020: Report of Special Rapporteur on right to privacy.
7. The U.N Resolution A/HRC/76/220 dated 23/7/2021: Report of Special Rapporteur on right to privacy.
8. The U.N Resolution A/HRC/49/55 dated 13/1/2022: Report of Special Rapporteur on right to privacy.

(E) THE DOCUMENTS AND THE INSTRUMENTS OF THE EUROPEAN REGION.

1. The European Convention on Human Rights, 1950 of the Council of Europe.
2. The Convention 108 of 1981 of the Council of Europe.
3. The Directive 95/46/EC of the European Union of 1995
4. The Charter of Fundamental Rights of the European Union, 2000.
5. The Regulation (EU) 2016/679 of the European Union (also called the General Data Protection Regulations) of 2016.
6. The Modernized Convention 108 (also called Convention 108+) of the Council of Europe.

(F) BOOKS

1. BAKSHI, P.M: THE CONSTITUTION OF INDIA, 17th Edition, 2020.

(G) NEWSPAPERS, REPORTS AND ARTICLES

1. Mandavia, Megha: 'The Personal Data Protection Bill, 2019 can turn India into "Orwellian State"- Justice B.N Srikrishna', article dated 31/1/2020 in Economic Times.
2. Macaskill, Eiven and Dance, Gabriel: 'NSA Files: Decoded.' the Guardian dated Nov.1 2013.

(H) BLOGS

1. Rizvi, Kazim : 'The Personal Data Protection Bill, 2019 and Surveillance : Balancing Security and Privacy' not dated, https://inc42.com

 [ISSN 2581-5369]

2. Khandekar, Omkar : 'Data Protection Bill can reduce the state's surveillance powers' article dated Aug. 15, 2020 in https://lifestyle.livemint.com
3. Agarwal, Aditi : 'NAMA : Issues Around Surveillance in the Personal Data Protection Bill, 2019' article dated Jan. 26, 2020 in https://www.medianama.com.

*****

 [ISSN 2581-5369]