GLC-SPIL International Law Journal

Students for the Promotion of International Law (SPIL), Mumbai

Volume II **Article 6**
2022

Short Article

Title:	Privacy in International Law: Where do India and Global South Stand?
Author:	Swaroop Nair

Recommended Citation:
Swaroop Nair, *Privacy in International Law: Where do India and Global South Stand?*, 2 GLC-SPIL INT'L L. J. 85 (2022).

PRIVACY IN INTERNATIONAL LAW: WHERE DO INDIA AND THE GLOBAL SOUTH STAND?

- *Swaroop Nair* [1]

ABSTRACT

In December 2021, Russia used its veto power against a resolution in the UNSC linking climate change and security. Now, that does not take the issue completely off the table. However, discussing climate change by expanding upon the Security Council's mandate of maintenance of international peace and security would be giving the powerful members of the Council the authority to dictate and decide on issues that affect different nations differently; it would essentially be antithetical to the entire purpose of the resolution. The idea here is not to completely dismiss the threat climate change poses to global peace and security; the idea, instead, is to direct the discourse towards realizing the double standards of the West and understanding the layered, disproportionate impacts on Global South when we talk about climate change and security. Hence, in that respect, the paper aims to understand the link between climate change and security by placing the interests of the Global South at the focal point.

INTRODUCTION

The goal of lawmakers is to structure long-term legislation in a world that is changing rapidly, and in no other field of law is this truer than in the field of technology and privacy. Privacy is widely accepted as a human right, and a major component of the right to privacy is the protection of data. In today's time and age, people's lives are practically controlled by their data and it is undoubtedly important that this data is protected from getting into the wrong hands. However, when we talk about breaches of privacy – like the time when Facebook shared the data of over eighty-seven million users with Cambridge Analytica[2], an incident that scared internet users all around the world, or even closer home in India, the leakage of private data of

[1] Student at Amity University, Mumbai

[2] Sam Meredith, *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*, CNBC (Apr. 10, 2018, 09:51 AM), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

hundreds of millions of Indians from databases of huge companies like Domino's or Air India[3] – we are not talking about one in a hundred, rarest of rare cases; breaches of privacy have become a rather common happening, and without any concrete legal framework set out to protect the data, to protect the privacy of individuals, the saying "privacy is a myth" will become true in every sense of the phrase.

India is home to the second-largest number of internet users in the world[4] and yet we do not have an extensive law formulated to protect the data of the citizens. The Parliament has been delaying the passing of the proposed Personal Data Protection Bill of 2018;[5] the multiple postponements can be attributed to the several complications in forming comprehensive data protection laws, which would be even more so complicated in a country as huge and diverse as India. As noted in the report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, India being a leading player in the "global digital landscape in the 21st century", there would be an added onus on the lawmakers of India because whatever law we create to protect the data of Indians, it should serve as a template for the Global South.[6]

In this paper, the concepts of privacy and data protection would be seen through the perspective of international law and how the Global South in general and India in particular stand in that regard. While considering the issues in the Global South with respect to privacy and data protection, this paper shall make an attempt to see those issues from a perspective that places India at the focal point. After this introduction, Section 2 of this paper seeks to first establish privacy as a human right in international law, taking the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights as the starting points for that discussion. Section 3 then looks at the need for comprehensive legal frameworks for data protection, which has become more relevant in today's global digital economy. Sections 4 and 5 then contrast the trends in the West to the trends in the Global South with respect to the right

[3]Vijaita Singh &Jagriti Chandra, *Data breaches expose emails, passwords of several government officials to hackers*, THE HINDU (Jun. 12, 2021, 08:03 PM), https://www.thehindu.com/news/national/data-breaches-expose-emails-passwords-of-several-government-officials-to-hackers/article34798982.ece.

[4]MeghaMandavia, *India has second highest number of Internet users after China: Report*, THE ECONOMIC TIMES (Sept. 26, 2019, 04:24 PM), https://economictimes.indiatimes.com/tech/internet/india-has-second-highest-number-of-internet-users-after-china-report/articleshow/71311705.cms?from=mdr.

[5]Yuthika Bhargava &Sobhana K. Nair, *More delays on Data Protection Bill as panel reopens debate*, THE HINDU (Sept. 07, 2021, 08:56 PM), https://www.thehindu.com/news/national/more-delays-on-data-protection-bill-as-panel-reopens-debate/article36344706.ece.

[6] Data Protection Committee Report, Available at, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

to privacy and data protection laws, and it also tries to understand the problems inherent in the Global South that stand in the way of protection of the right to privacy. Finally, the concluding section, after making a study of the aforementioned areas, tries to determine the way forward.

I. PRIVACY AS A HUMAN RIGHT IN INTERNATIONAL LAW

That the right to privacy is a fundamental human right is widely accepted by the International community – the provisions of two of the most important documents in the history of human rights, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (to both of which India is a signatory), firmly establish that.

Article 12 of the UDHR reads as follows:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[7]

Article 17 of the ICCPR reads as follows:

> *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks."*[8]

Furthermore, it is also the Human Rights Committee, the aim of which was to interpret and implement the provisions laid down in the ICCPR, which gave the General Comments on specific issues covered in the Covenant. Out of them, General Comment 16 provides us with a deeper analysis and interpretation of Article 17; it recognizes that:

> *"The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized*

[7] Universal Declaration of Human Rights, 1948, art. 12.
[8] International Covenant on Civil and Political Rights, 1966, art. 17.

by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his privatelife, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Everyindividual should also be able to, ascertain which public authorities or private individualsor bodies control or may control their files. If such files contain incorrect personal data orhave been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."[9]

In addition to that, the term privacy also finds mention in Article 16 of the Convention on the Rights of the Child[10] and Article 14 of the International Convention on the Protection of All Migrant Workers and Members of Their Families.[11]

Furthermore, the United Nations General Assembly adopted several resolutions on the right to privacy in the digital age, first in 2013, then in 2014, 2016 and 2018. These resolutions reaffirmed the right to privacy, both online and offline and called upon States to take appropriate measures to protect the right to privacy.

And that is the interesting part; the term privacy finds mention in many international treaties and conventions, yet until recently, it was not at the forefront of legal policies.[12] However, with the advancement of technology and the realization of the worth of personal data and the importance of privacy, throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection.

Now the aim of international human rights law is that it attempts to adapt the practices of local cultures so as to bring them in line with the universally accepted principles of human rights.[13] In that regard, over one-hundred-and-thirty countries, directly or indirectly, have constitutional

[9]UN Human Rights Committee (HRC), *General comment no. 16, Article 17.*
[10] UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3
[11]UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, A/RES/45/158
[12]Kristian P. Humble (2021) *International law, surveillance and the protection of privacy*, 25 THE INT'L J. OF HUMAN RIGHTS, 1-25 (2021).
[13]Tom Zwart, *Using Local Culture to Further the Implementation of International Human Rights: The Receptor Approach*, 34 HUMAN RIGHTS Q. 546-569 (2012).

statements regarding the protection of privacy.[14] In India too, in what is considered to be a landmark judgement, Article 21 of the Indian Constitution[15] was interpreted by the Supreme Court in the *Puttaswamy case* to include the dimension of the right to privacy as an important aspect of living with dignity.[16] Often considered to be the most important fundamental right, the meaning of Article 21, which is in consideration here, is incomplete without the aspect of dignity. Within the rights which humans need to live a life of dignity comes the right to privacy too; to be able to keep certain information secret from others is fundamental to protecting oneself. It would, thus, not be wrong at all to say that "the right to privacy is considered to be an identifiable human right with universal qualities deserving legal recognition and protection, although the scope of such legal protection is still being determined."[17]

II. THE NEED FOR LAWS THAT PROTECT DATA AND PRIVACY

While dealing with the concept of privacy and the continuous advancement of new technologies, it can make anyone question what level of protection of our right to privacy is possible in a world where personal information of more or less any person can be accessed by just a click or the press of a button. New technologies in the form of the internet, social networks, remote access to information, etc., though they bring the whole world at our fingertips, make it increasingly more difficult to maintain privacy rights in cyberspace such that online invisibility has become next to impossible. In this context, it has become increasingly important that there are rules that protect privacy. The presence of such rules would give us the ability to strengthen our rights in the face of significant power imbalances. The right to privacy is important for us to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us while protecting us from others who may wish to exert control. In fact, in the larger scheme of things, privacy could be considered not simply as an individual right, but as a collective right. But obviously, the right to privacy, like any other right for that matter, is not absolute. States may lawfully restrict an individual's rights in order to protect the rights of others, the general

[14]PRIVACY INTERNATIONAL, (last visited: Sept. 29, 2021), https://privacyinternational.org/explainer/56/what-privacy.
[15] INDIA CONST. art. 21.
[16] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[17] Alexandra Rengel, *Privacy as an International Human Right and the Right to Obscurity in Cyberspace*, 2 GRONINGEN J. INT'L L. (2014).

welfare, public order, morality and the security of all. In doing so, States may not take out the entire essence of what the term privacy encompasses.

Hence, in order to protect the right of privacy of individuals, particularly in cyberspace, the need of the hour is a concrete data protection law. And the mammoth question that presents itself in front of academicians and lawmakers is what would such a concrete data protection law entail.

In the Indian context, the judgement of the Supreme Court of India in the case of *People's Union for Civil Liberties (PUCL) v. Union of India*[18] set us on the path of recognizing the importance of the right to privacy. And then further in the landmark judgement in the *Puttuswamy case,* the right to privacy was rightly held to be a fundamental right "flowing from the right to life and personal liberty as well as other fundamental rights securing individual liberty in the Constitution".[19]The rationale behind upholding the right to privacy as a fundamental right can also be seen from the perspective of individual dignity – to protect their identity, a person must be free to retain or share their data with their consent. "This core of informational privacy, thus, is a right to autonomy and self-determination in respect of one's personal data. Undoubtedly, this must be the primary value that any data protection framework serves."[20]

III. TRENDS IN THE WEST IN CONTRAST WITH THE TRENDS IN THE GLOBAL SOUTH

The Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, set up to deliberate on a data protection framework,[21] noted at the beginning of their report that broadly there are three approaches to data protection.

The two most popular approaches to data protection are the approaches of the United States of America and that of the European Union. In the United States of America, a *laissez-faire* approach is followed; courts of law in landmark cases like *Roe v. Wade*[22] and *Griswold v.*

[18] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[19] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[20] Data Protection Committee Report, Available at, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[21] *Justice Krishna to head expert group on Data Protection Framework for India*, PRESS INFORMATION BUREAU GOVERNMENT OF INDIA (Aug. 01, 2017), https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420.
[22] Roe v. Wade 410 U.S. 113 (1973).

Connecticut[23] have interpreted constitutional provisions laid down in the First, Fourth, Fifth and Fourteenth Amendments to their Constitution[24] to recognize the right to privacy that protects the citizens against the federal government and also against the private sector.

When the European Union enacted the General Data Protection Regulation (henceforth, EU GDPR)[25], it was seen as a milestone for data protection standards.[26] The EU GDPR is a rather comprehensive set of regulations that keeps the protection of personal data and the right to privacy of individuals at the forefront; it does indeed look like a promising set of regulations that places the consumers before the corporations.[27] Even as a regulation, and not as a directive, it served as a model that several countries, even outside the European Union, adopted to protect the personal data of individuals.

China has the third approach to protecting data; the nation has approached the issue of data protection "primarily from the perspective of averting national security risks".[28] Although there seems to be "a growing convergence between Europe and China's approaches in emerging data protection regimes", China's new national standard on personal information protection looks more stringent than even the EU GDPR.[29]

Now, of course, the policies of the Western States cater to their own interests, and China's, the other major point of power, which has its own interests that are reflected in its own policies. As the committee report further remarks, India's interests are not exactly coincidental with thatof the three aforementioned legal regimes. And this is generally true for the Global South. The cultural and political scenario in the Global South presents its own new dimension of data protection related issues which cannot simply be dealt with by Western legal frameworks. Crimes over and through the digital landscape have increased in the Global South but the "concepts of privacy and citizens' corresponding political rights have not been well-developed

[23] Griswold v. Connecticut 381 U.S. 479 (1965).
[24]U.S. Const. amend. I, IV, V, XIV.
[25] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[26] J. Albrecht, *How the GDPR Will Change the World*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 287-289 (2016).
[27]Payal Arora, *General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South*, 17 SURVEILLANCE & SOCIETY (2019).
[28] Data Protection Committee Report, Available at, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[29]Samm Sacks, *New China Data Privacy Standard Looks More Far-reaching than EU GDPR*, CENTRE FOR STRATEGIC AND INTERNATIONAL STUDIES (Jan. 29, 2018), https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.

in non-Western contexts".[30] And that is a chief reason why the United Nations Conference on Trade and Development reported that a good fraction of nations around the globe lack proper legislation for data protection.[31]

And has thus become relevant to the old academic debate on "universalism versus particularism". As is true for almost any other aspect of the law, privacy-related problems in the Global South cannot be seen through the eyes of the developed West. While acknowledging that the universally accepted documents like the UDHR and the ICCPR (which also have shades of Western legal and political thought) do lay down the basic idea, the Global South cannot have data protection laws modelled after Western views and institutions.

IV. PRIVACY RELATED ISSUES IN THE GLOBAL SOUTH

Today's digital economy is vastly data-driven. This gives immense potential to India and other countries in the Global South to embark on the path of empowerment, development, progress and innovation.[32] However, just as much potential it has to empower, data has equal potential to harm; it comes with its own set of risks and it can create new dimensions of inequalities and injustices.

Data protection is in its own regard a complicated topic of law, framing a legal policy for which would be an intersection of national security with technology, a cobweb of power dynamics, innovation and regulation. On one hand, the personal data of individuals is viewed as a strategic state resource and this view comes in conflict with the idea of privacy. The discourse on privacy, data and law transcends that as we span cultural backgrounds. What is implied here isthat there are vast differences when we compare issues related to privacy in the developed Westand in the Global South. So, when we add to that discourse the other economic, social, culturaland political problems, the already existing problems related to data privacy then look more pronounced in the Global South.

[30]Ahmed, Syed Ishtiaque& Haque, Md & Guha, Shion& Rifat, Mohammad Rashidujjaman& Dell, Nicola. (2017). *Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh*, CHI 906-918 (2017).

[31] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited Sept. 29, 2021).

[32] GERALDINE BASTION & MUKKU, SREEKANTH, DATA AND THE GLOBAL SOUTH KEY ISSUES FOR INCLUSIVE DIGITAL DEVELOPMENT 7 (Heinrich-Böll-Stiftung 2020).

However, when we say most countries outside the West have lax or no privacy laws,[33] the reasons behind it are multifaceted. For one, privacy concerns may be compromised in the Global South for the sake of more pressing needs like economic and social development. So, while in a more developed region like Europe, users have a seemingly legitimate and comprehensive legal framework in the form of the EU GDPR to protect them against privacy violations, the citizens of the Global South are at a greater risk of indiscriminate data surveillance because their governments are fighting other battles at the same time. This takes them farther away from having corporations and governments move toward governance rooted in universal human rights. And then there is also the other perspective – many governments in the Global South rule by the law while being above it – extensive privacy laws would not facilitate these authoritarian elites in power to weaponize laws against their people to sustain their regimes.[34]

In the Indian context too, there are multiple challenges that pose themselves before lawmakers in the process of framing a comprehensive data protection legal framework. As Honourable Justice Chandrachud noted in the *Puttuswamy case*,

"Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State."[35]

The Supreme Court of India held that Indian citizens are protected from the State's invasion of privacy unless done by the least restrictive means. To that end, a compressive data protection law is the need of the hour. If we are to have a law for data protection, then it would not be ideal if such a law would give unprecedented powers to the bureaucratic apparatus. The proposed bill for data protection needs a few things to be addressed. It has to protect personal data and non-personal data. It has to place emphasis on consent, in theory, and in practice. If there is data gathering for legitimate purposes, then it should be more transparent. More importantly, there must be an independent system of checks and balances that individuals can

[33]TAYLOR, LINNET & FLORIDI, LUCIANO & SLOOT, BART, GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (Springer 2017).
[34]Payal Arora, *General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South*, 17 SURVEILLANCE & SOCIETY (2019).
[35]Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

resort to if their data is compromised and their right is violated. The State cannot be left to *de facto* encroach upon the data that is out there in public domains.

V. THE INDIAN APPROACH

It has been over four years since the *Puttuswamy* judgment affirmed the Constitutional right to privacy and the key issue of protection of personal data of individuals has not yet been legislated upon and codified in a strong, comprehensive set of laws. The proposed Personal Data Protection Bill, which was tabled in Parliament in 2019, has several issues pertaining to it and several controversies surrounding it, which all need to be addressed before it is passed and enacted as an act of Parliament and consolidates the individual right to privacy.

The criticisms against the proposed bill start right from the composition and the working of the Justice Srikrishna Committee that was tasked with examining its nuances. The working of the committee has to be questioned because of the lack of social participation and lack of transparency in its working.

In theory, it emphasizes consent – ideally individuals are vested with the right to know and deny access to their data – but a major point of concern with this proposed bill is how its provisions seem to be favouring the interests of corporate and/or non-corporate entities by enabling them to exploit personal data of individuals and use it against them. Moreover, even though the government has been given the power to process data of individuals for "functions of the State", there is not really a system of checks and balances when the government is allowed to use data without consent. Indeed, there is the provision for the establishment of the Data Protection Authority, a regulatory agency tasked with the regulation of the use of personal data across sectors. However, there are serious qualms about the independence of the agency[36] because its appointment is bound by the Central Government and it is not even mandatory for it to constitute at least one independent expert or a member of the judiciary on its governing committee, an issue that was raised in the reports of the Joint Parliamentary Committee. Although the very fact that the draft bill was sent to a Joint Parliamentary Committee instead

[36] *#StartFromScratch: Why is the data protection bill being criticized?*, Internet Freedom Foundation, https://internetfreedom.in/why-is-the-data-bill-being-criticized/

of following the traditional route of it being examined by the Standing Committee on Information Technology was a questionable decision taken by the legislators, the report of the JPC did indeed address quite a few of the concerns earlier raised when the draft bill was proposed; however, even if the recommendations are taken into consideration, it does not still fully provide for a strong safeguard for the protection of data of individuals.[37]

The legal atmosphere surrounding privacy in India is more or less in a state of quagmire. Several pieces of legislations that are being enacted or that are going to be enacted have the common problem of being characterized by imprecise language, arbitrary content legislation and requirements of traceability and decryption to questionable extents. This is true not only inthe case of the proposed Data Protection Bill but the notorious intentions of the authorities canbe seen in the introduction of the IT Rules[38], the controversies surrounding the alleged procurement of the Pegasus spyware from the Israeli NSO group[39], the Indian law enforcement's increasing reliance on artificial intelligence (AI) and facial recognition technology in recent times in an unregulated manner[40], all of which could pose a potentially dangerous threat to citizen's right to privacy by giving rise to surveillance by State.

The current government and the Prime Minister's goals of Digital India and the country becoming a $5 trillion economy[41] need "innovation, aspiration and application of technology" as driving forces to fuel it. The ambitious movement towards a digital economy as envisioned by the government is deemed to be important to improve lives, and indeed, data has the potential to do that. However, in this technology-driven era and in this ecosystem of big data,

[37]Pallavi Bedi, *What the JPC Report on the Data Protection Bill Gets Right and Wrong*, THE WIRE (Dec. 20, 2021), https://thewire.in/tech/what-the-jpc-report-on-the-data-protection-bill-gets-right-and-wrong.
[38]*IT Rules 2021 add to fears over online speech; critics believe it may lead to outright censorship*, FIRSTPOST (Jul. 16, 2021, 12:17 PM), https://www.firstpost.com/tech/news-analysis/it-rules-2021-add-to-fears-over-online-speech-privacy-critics-believe-it-may-lead-to-outright-censorship-9810571.html#:~:text=Many%20other%20critics%20say%20Modi's,will%20benefit%20and%20empower%20Indians .
[39]The Hindu Bureau, *Opposition slams Government as New York Times report says India bought Pegasus spyware*, THE HINDU (Jan. 29, 2022, 11:33 AM), https://www.thehindu.com/news/national/pegasus-and-a-missile-system-were-centerpieces-of-2-billion-deal-between-india-and-israel-in-2017-nyt/article38343251.ece.
[40]Jai Vipra, *The use of facial recognition technology for policing in Delhi*, VIDHI CENTRE FOR LEGAL POLICY (Aug. 16, 2021), https://vidhilegalpolicy.in/research/the-use-of-facial-recognition-technology-for-policing-in-delhi/.
[41]*India poised to become $5-trillion economy by 2024-25: Puri*, ECONOMIC TIMES (Oct. 21, 2021, 05:08 PM),https://economictimes.indiatimes.com/news/economy/indicators/india-poised-to-become-5-trillion-economy-by-2024-25-puri/articleshow/87185563.cms?from=mdr.

the privacy of Indian citizens cannot be compromised. The Centre in several areas of legislation has strongly said that it cannot blindly follow the West. It is indeed true in the case of privacy and data protection, however, the current approach taken by our country's legislators is not adequate enough to safeguard the interests of the Indian public. The need of the hour is the enactment of a strong data protection law, but it does not mean that a shoddily crafted bill giving unprecedented powers to the bureaucratic apparatus be imposed, that would not meet constitutional standards if taken to Court and be eventually struck down. The urban-rural divide, the digital gap, and rampant discrimination on various constitutionally barred grounds are not unrelated matters in the discourse on privacy and data protection. Without taking into account these pressing matters, we cannot have a good law enacted to protect the data of individuals.

CONCLUSION

Although it is a relatively newer idea, the right to privacy is a fundamental human right – the UDHR and the ICCPR, as we have seen, establish that firmly. Nations agreed to protect this right in resolutions of the United Nations General Assembly and in addition to that, many of their Constitutions also reflect that. For the right to privacy to not lose its essence, it is essential that there be a comprehensive set of regulations, and a solid legal framework to protect the data of individuals. Undoubtedly, this is a complicated faction of law, which, in practicality, becomes even more so complicated in the Global South. The nations in the Global South have their battles to fight, which, in essence, are vastly different from the experiences of the West. It would, hence, not be appropriate to impose the same set of data protection regulations applicable in the developed West on the nations that constitute the Global South. The approaches of neither the United States of America, the European Union, nor China would be fit for the situations prevailing in the Global South. That is not to say that these approaches are not sound sets of regulations; in fact, they do offer a source of inspiration. Perhaps a combination of these three approaches along with newer ideas put on the table can yield a framework of data protection laws suitable for the Global South. The Global South needs its own model of a data protection law that "protects individual privacy, ensures autonomy, allows data flows for a growing data ecosystem and creates a free and fair digital economy". India has the opportunity to lead the way for the Global South – India can pave the way for governance that respects individual autonomy and universal human rights.