ISSN 2249 - 1430

NIRMA UNIVERSITY
INSTITUTE OF LAW
NAAC ACCREDITED 'A' GRADE

NIRMA UNIVERSITY LAW JOURNAL

# NULJ

Volume - XI

Issue - I

December 2021

## Articles



## Policy Brief



## Book Review

# NIRMA UNIVERSITY LAW JOURNAL
# NULJ

*Bi-Annual Referred Journal*

**ISSN 2249 – 1430**

**Volume XI • Issue I • December 2021**

# FOREWORD

*I am pleased to present before you all Volume -XI Issue – I December, 2021 Nirma University Law Journal (NULJ) Peer reviewed and Referred Journal. The Journal is dedicated to highlighting legal and interdisciplinary research, policy brief and contemporary case comments. I am happy to share that the article which have been published in this Journal it is indexed to Manupatra and SSC online. The overwhelming response we received from contributors for the publication of this Volume XI, Issue I which was theme-based 'Law, Society and Technology in 21st Century'. The selected research articles with Interdisciplinary in the categories of research article, policy brief and book review.*

*The veritable contributions are indicative of the efforts and ingenuity of the author, the academic and practical impact on the reader its must be credited to the qualitative and insightful writings of authors. On behalf of the Nirma University, I congratulate the authors for maintaining the highest standards academic honesty and purity in thoughts.*

*We feel extreme pride in being a medium of expression the broadcasting novel ideas being a crucial platform for legal, interdisciplinary and contemporary legal discourse.*

***Dr. Madhuri Parikh***
*Chief Executive, Nirma University Law Journal*
*Director and Dean I/c*
*Institute of Law, Nirma University*

## *TABLE OF CONTENTS*

### Articles



### Policy Brief



### Book Review

# DATA PRIVACY IMPLICATIONS OF CONTACT TRACING APPS IN INDIA

Monica Shaurya Gohil*
Dr. Chetna Bujad**

**ABSTRACT**

*In the year 2020, the entire world stood still, and everyone stayed put in the four corners of their homes to be safe whilst deadly pandemic played havoc everywhere. The pandemic has not shown signs of abating in the following year too. One of the widely accepted strategies to combat Covid-19 has been contact tracing. Many governments around the world introduced contact tracing mobile applications ('apps') that could trace an infected person and warn others who have been in his or her vicinity about such a case, so that they may isolate themselves and take adequate precautions to check the advancement of the disease. To avail the facilities of these apps one had to feed his/ her personal information into the app. Although a very strong case is made for its assistance in managing the pandemic, there are obvious privacy implications on the process of collection and management of data by such Apps. This article tries to evaluate what kind of personal data these apps collect and store and to weigh in their benefits vis-à-vis the implications of contact tracing on the right to data privacy.*

* Advocate High Court of Gujarat & Research Scholar, School of Law, Gujarat University. The author can be contacted at monicagohil@gmail.com.
** Assistant Professor, School of Law, Gujarat University. The author can be contacted at chetnavyas3@gmail.com.

***Keywords:*** *Covid-19, Pandemic, Contact Tracing, AarogyaSetu App, Right to Privacy, Data Protection*

## I. INTRODUCTION

The world learnt many a lesson from the deadly pandemic which engulfed the entire mother earth simultaneously. With the help of technology, the government along with the health sector tried their level best to provide the best possible solutions to prevent the infected from spreading the disease further. Technology was leveraged, as it should in the information age to assist in this endeavour. One such technology was the development of mobile apps which were designed to identify an infected person. On April 2, 2020, India too jumped on board and unveiled AarogyaSetu, a homegrown contact tracking app. On May 11, 2020, vide an order the Indian government notified its citizens to download the app and empowered the National Informatics Centre (NIC) to collect, process, and store data thus collected by the said App.[1] By making it compulsory for travel, physical attending of offices by both public and private employees the government exhorted every Indian citizen to download the AarogyaSetu App. It collects demographic, location, contact and self-assessment data collectively called "response data".[2] By tracking the movement of people and utilizing their personal data to spy not only on the infected but innumerous others who were not infected, the authorities infringed on the constitutionally protected right to privacy and data protection and also the right to be left alone[3]. Right to private life and personal privacy are rights that cannot be meddled with, without satisfying the legality of such action.

Considering that India currently lacks data privacy laws, regulating such techniques for collecting information by the state and corporate entities is extremely challenging. No doubt unusual situations call for drastic measures

[1] Government of India*, The AarogyaSetu Data Access and Knowledge Sharing Protocol* (2020), https://static.mygov.in/rest/s3fs-public/mygov_159051652451307401.pdf.

[2] *Id* at 1.

[3] Danny Palmer, *Coronavirus contact-tracing apps: What are the privacy concerns?*,ZDNET, (April 14, 2020), https://www.zdnet.com/article/coronavirus-contact-tracing-apps-what-are-the-privacy-concerns/ (last visited on: September 1, 2021).

but without any legal backing, the act of collection of personal data without specifying the duration for which such data is being collected and for whom exactly is it being collected gives rise to serious privacy concerns among people. In absence of legislation to this effect, each and every government-initiated activity must pass "the three-fold test"[4] stated by the Hon'ble Supreme Court in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors*[5], also known as the 'Privacy Judgement'.

The Three-fold test to analyze whether State action violates the privacy rights of the citizens is–

a. Is there a legal backing to any action taken by the State?

b. Is there a dire need that can legitimize the action taken by the State which infringes the privacy rights of the citizens?

c. Is the amount of data collected consistent with the level of the ensued exigency?

There exists no legal backing because the country lacks a legal and regulatory framework for data protection and data privacy that can empower the government to collect such humungous data in the name of pandemic management. Thus, the State needs to justify its actions and also specify the proportion of data so collected is consistent with the need for such action.[6] Under the Disaster Management Act of 2005, the government has taken a number of steps to combat the proliferation of corona virus in the country over the last year and a half. The purpose of imposing the first test of legality by the Hon'ble Supreme Court was to keep a check on the actions taken by the government by a mere executive order in drastic times which may violate people's privacy rights. However, there exists a valid debate as to invoking the Disaster Management Act fulfils the legality test of *Puttaswamy* judgment or not, more so when there is no clear and declared policy on the storage and management of such data.

[4] Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.,v(2017) 10 SCC 1.

Since it is for the first-time governments around the world have taken a resort in the usage of technology to combat a pandemic situation there are no prior precedents on which we can rely to evaluate the actions of the government vis-à-vis privacy violations. This paper thus attempts to examine the working of contact tracing apps; what kind of data they collect and whether making the use of such apps mandatory is in violation of the privacy rights of the citizens guaranteed by the Constitution of India.

## II. EVOLUTION OF RIGHT TO PRIVACY IN INDIA

When technological advancements were picking pace in most parts of the world India was still under the colonial rule of the British Empire. Even when the new technologies finally reached the subcontinent it was mainly used by the British for their work. Later after independence too, Indians never felt an immediate threat to their privacy from such technologies as the country had a much larger work at hand then, of '*Nation Building*'. As a result, for unclear reasons, privacy rights were not provided as a basic right to the citizens by the framers of the constitution, due to which privacy as a fundamental right has been fighting for its recognition since the 1960s in India. The first casual mention of it in Indian courts was in 1954 in the case of *M. P. Sharma v Satish Chandra*[7] where the issue was if "search and seizure "during an investigation conducted by the government officials violated a person's right against "self-incrimination". After a thorough analysis of developments around the world, the right to privacy was not acknowledged as a constitutional right by the Supreme Court. The Court reasoned its decision as:

> "……when the Constitution makers have thought fit not to subject such regulation to Constitutional Limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it into a totally different fundamental right."[8]

---

[5] *Id.*

[6] VrindaBhandari& Karan Lahiri, *The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World*, 3(2) UNIV. OF OXFORD HUMAN RIGHTS HUB JOURNAL, 15 (2020).

In 1963, in *Kharak Singh v State of Uttar Pradesh*[9] the intervention of the court was sort once more to safeguard the right to privacy. Perhaps for the very first time probably, the Supreme Court deliberated on this topic in depth. Kharak Singh who was released in a robbery case was marked for surveillance and was from time to time picked from his home by the police, who constantly kept a watch on his whereabouts despite him not being convicted for the crime. Tired of such scrutiny at all times, he approached the court on the grounds that his liberty is being jeopardized by the police. The case was heard by a bench of six judges. Except for Justice Subba Rao, who dissented, the rest of the five judges held that the right to privacy is not recognized by the Indian Constitution as a constitutional right, hence no fundamental rights of Kharak Singh were violated.

For over a decade after the Kharak Singh case, the Supreme Court did not get an opportunity to rethink its limited perspective regarding privacy. It was in 1975 in *Gobind v State of Madhya Pradesh*[10] that privacy violation as a bone of contention came to the fore all over again. Both the Kharak Singh case and the Govind case were somewhat similar as both petitioners challenged the Police Regulations. Govind was a convicted criminal and was put under surveillance by the M. P. Police. He, too, alleged that the government's surveillance of his travels and visits to his home infringed upon his right to life and liberty guaranteed by Article 21 of the Constitution. Being a smaller bench, the court, in this case, could not overrule the judgment of the Kharak Singh case. However, Justice K. K. Mathew did take a note of the changing times and opined:

> "……Of Course, privacy primarily concerns the individual. It, therefore, relates to and overlaps with the concept of liberty. The most serious advocate of privacy must confess that there are

[7] (1954) SCR 1077.
[8] M. P. Sharma v Satish Chandra, (1954)SCC 24.
[9] (1964) 1 SCR 332.
[10] (1975) 2 SCC 148.

> serious problems of defining the essence and scope of the right……"[11]

Justice Mathew referred to *Wolf v Colorado*[12]a case decided in the US and pointed out that the privacy rights of any person against any type of intrusion by the police must be safeguarded in a similar way, as it is done in the US.

Although the right to privacy was not regarded as a basic right in the Gobind case per se, it did open the floor for debates on this issue and several cases were decided by the Indian courts forming a solid base for privacy jurisprudence in the country. The courts adjudged a variety of issues being it medical privacy[13], rights of the press[14], prisoners' rights, rights of a rape victim[15], telephone tapping[1617]etc. In each case, the courts referred to the prior three judgments and particularly the stance taken by the court in the Govind case.

Finally, it was in 2017 in the case of *Justice K S Puttaswamy (Retd.) and Anr. v. Union of India and Ors*[18], while deciding on the privacy issues relating to Aadhar that the nine-judge bench stated unequivocally that the right to privacy is a basic right enshrined in Article 21, which grants people of India the right to life and personal liberty. Justice Chandrachud along with other judges on the bench overturned the rulings in the M. P. Sharma and Kharak Singh cases, which did not recognize personal privacy as a constitutionally protected right and declared:

> "Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article

---

[11] *Id* at 23.
[12] (1949) 238 US 25.
[13] Bhabani Prasad v Orissa State Commission for Women, AIR 2010 SC 2851.
[14] R. Rajagopal v State of Tamil Nadu, AIR 1995 SC 264.
[15] ABC v Commissioner of Police, W.P (C) 2005.
[16] AIR 1997 SC 568.
[17] (2011) 7 SCC 69.
[18] *Supra* note4.

> 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III."[19]

The nine-judge bench opined that the growth of technology and its uses could prove to be devastating if adopted blindly. They recognized the need for technology for good governance but were also mindful of the privacy issues that tag along with such technologies. There must exist a balance while implementing such technologies which may, in turn, benefit both the government and people without violating their privacy rights.

## III. IS PRIVACY AN ABSOLUTE RIGHT?

The debate now is whether the right to privacy is a constitutional right or an absolute right. The answer is no, the right to privacy is not unalienable. It is subject to restrictions that are imposed through a practical, rational, fair, and just procedure of law that must not be tyrannical, autocratic, and despotic.[20] Justice Chandrachud in the Puttaswamy case opined that just like the other rights provided by the Constitution in Part III, the right to privacy is also not an absolute right and can be interfered with in certain circumstances. However, any such interference by the State must "satisfy the test of reasonableness of restriction" under Part III.[21] Further, Justice Chelameswar opined that no legal right is absolute and may be regulated by the nature of such right. According to Justice A. M. Sapre, if according to the State there exists a "social, moral and compelling public interest", the State is lawfully sanctioned to restrict the right to privacy in such circumstances.

In light of the learned judges' conclusions in the *Puttaswamy* case, it is reasonable to conclude that, while the right to privacy is a guaranteed right, it is not an absolute right. Like the other rights under Part III, even the right

---

[19] *Id* at T and 3(C).
[20] Maneka Gandhi v UOI, AIR 1978 1 SCC 248.
[21] *Supra*note4.

to privacy is limited and can be restricted if the action taken by the State passes the test of reasonable restriction.

## IV. AAROGYA SETU APP: BOON OR BANE?

After the World Health Organization proclaimed thespread of corona virus a global pandemic on March 11, 2020, all governments around the world tried their level best to control the situation. For months, many countries, including India, implemented state-wide curfews. Travel across national borders, as well as within a country, was limited. Symptomatic people were tested, contained, and treated in isolation centres. All required precautions were taken to prevent the uncontrolled spread of a life-threatening illness, which might wreak havoc on the already overburdened public health system. In these difficult times, the use of technology came very handily, and contact tracing applications were adopted by various countries to track and contain the infected. The National Informatics Centre (NIC) created and launched the AarogyaSetu, a contact tracing app as their weapon to combat the proliferation of COVID cases, in India. However, it raised compliance concerns in the country when the Indian government made it compulsory for every citizen to install the app on their mobile phones. Many had concerns that such technologies used during such extraordinary situations may become 'tools of mass surveillance' later. The government's approach, according to Justice B. N. Srikrishna, Head of the Committee that prepared the Personal Data Protection Bill, was "utterly illegal "with no legal backing to it.[22] Hence, cropped up the issue of privacy violation by such apps. In comparison to managing health crises and safeguarding privacy, no doubt the former is of foremost importance. However, many believe that even in such extraordinary times government cannot infringe the privacy of its citizens disproportionately.

[22] Apurva Vishwanath, *Mandating use of AarogyaSetu app illegal*, INDIAN EXPRESS, (May 13, 2020), https://indianexpress.com/article/india/aarogya-setu-app-mandate-illegal-justice-b-n-srikrishna-6405535/ (last visited on September 14, 2021).

**Data Collected by the App**

The AarogyaSetu App gathers the following kinds of data at the time of registration:

a) Demographic Data – includes the name, gender, age, mobile number, occupation, and history of travel.

b) Location Data - collects the precise location of the person via GPS along with Bluetooth.

c) Contact Data -with the help of Bluetooth services tracks every movement of the person including whom such person has had proximity within the recent past.

d) Self-Assessment Data - the responses a person has provided to a test/questions in the app.

The app is supposed to collect and preserve information of every individual a person meets to inform them in case such person is tested positive for COVID-19. This in turn warns others who were physically in close proximity of such person to get tested and isolatethemselves in order to avoid infecting others.This information remains on the "device by default"and is only extracted and stored on a government server if a person tests positive to "formulate appropriate health response".[23]

**Apportionment of Response Data**

The NIC is authorized to share the personal data thus collected with the "Ministry of Health and Family Welfare, Government of India, Health Departments of various States or Union Territories or Local Governments, and National or State Disaster Management Authorities".[24] The Government protocol also mentions that such data in 'de-identified' form may be shared with universities or institutes for research purposes.

[23] *Supra* note 1, 5 at 2.
[24] *Id.*

**Privacy Concerns surrounding the App**

All contact tracing apps around the world use two types of approaches to collect and analyse the data – the centralized and decentralized approach. A centralized approach collects and stores data on government servers that can be accessed by the government and health departments. In this approach not only the anonymized ID of the infected person is uploaded to government servers after such person updates his or her health status but also codes of such other persons the infected has come in contact with. On the other hand, in decentralized approach personal data of a person remains on his or her device only and minimal data is accessed by the government and its concerned authorities. Here the phone only shares an anonymized ID with the government authorities. An interface released by Apple-Google known as Exposure Notification System (ENS) claims to use the decentralized approach. The ENS detects other devices that have been in close proximity of an iPhone or Android phone for a significant period and then create a uniquely identifiable code. This code is stored in encrypted form on both the original device and the devices such device has come in contact with. If one updates information about being infected, that information, together with all unique identification codes, is transferred to an app server. Information of the other persons that the infected person has come in contact with remains on their phones only and is not 'de-identified' and only information of an infected person is 'de-identified' by the central server.[25]

Initially when the pandemic outbroke most countries used the former i.e., the centralized approach. Countries like China, South Korea and Singapore claimed to have significantly minimized the spread of the disease with the help of their contact tracing apps. In particular, Singapore's TraceTogether was considered to be a great success which encouraged other countries to work on similar lines. India's AarogyaSetu app too works on a centralized

[25] *Apple/Google Exposure Notification: Cryptography Specification*, (April 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf (last visited on September 21, 2021).

approach. Here personal data of the infected person and others, such person has come in contact with is collected and stored on government servers and shared with government health authorities and other local authorities.

AarogyaSetu app collects both GPS and Bluetooth data along with other personal data which undermines global data privacy standards of data minimization. Such humungous data in the hands of the government raises serious concerns about privacy violations, data breaches, vulnerabilities of citizens and to a great extent profiling of citizens. With no legislation regulating the use of data in India, there exists minimum accountability on the government as AarogyaSetu app users are at the mercy of privacy policy framed by the government. Reportedly, due to security and privacy concerns, the Indian army directed its personnelnot to use the app in sensitive locations, cantonments and other areas of operation and switch on their location tracker and Bluetooth in public places or while visiting isolation centres only.[26]

Furthermore, there is little clarity or transparency as to who has access to the app's data. According to the government's privacy policy, it can be shared with government health agencies and other local entities. It may also be shared with research centres and universities for scientific research purposes. However, the app isn't based on the 'privacy-by-design' concept of global standards. Google server hosts the AarogyaSetu App and Amazon Web Services is the host for the app data. This creates concerns that users' sensitive data is not only with the government authorities but also private players like Google and Amazon. Thus, the privacy policy is vague and unspecific regarding the sharing of app data too.

The app does not take informed consent from users to share their response data. On January 25, 2021, a division bench of the Karnataka High Court

[26] Amrita Nayak Dutta, *Army advises personnel to use govt's AarogyaSetu app, but with usual cyber precautions,* THE PRINT, (April 15, 2020), https://theprint.in/defence/army-allows-personnel-to-use-govts-aarogya-setu-app-but-with-usual-cyber-precautions/402527/ (last visited on September 26, 2021).

passed an interim ruling in a writ petition[27] restraining the government and NIC from sharing the response data of users collected by the AarogyaSetu app without taking informed consent from them. Because the AarogyaSetu Data Access and Knowledge Sharing Protocol, 2020 is not included in the app's terms of service or privacy policy, the court concluded that there is no informed consent from app users for the sharing of their response data as described in the protocol.

Apart from legal issues there also exist technical issues with the app. Unlike Apple-Google ENS which generates digital codes that are constantly changing, the unique identity code the AarogyaSetu app generates is a static number. Being a fixed code increases the chances of a person being identified thereby violating his or her privacy. The government initially refused to release the app's source code because it was a "non-open-source" application. However, after facing a backlash from privacy advocates source code of the app was released. Interestingly, this code was of the prior version of the app, and not that of the upgraded one. Hence the app's 'server-side-code' was not made available at all, resulting in a lack of transparency regarding the app's operation.[28]

Another major concern of the use of technology during the pandemic is that these measures taken as extraordinary interventions to fight the pandemic may later become permanent and empower the government to intrude in the lives of the people and use such technologies for mass surveillance. Even the application's privacy policy does not mention that it is a temporary measure undertaken only for the pandemic. Hence, suggesting that government could use the application later too if it desires to make the AarogyaSetu app a genesis of constant surveillance.

Unlike the EU, which has provided its citizens with a comprehensive and rigorous data and privacy protection policy in the form of the General Data Protection Regulation (GDPR), India lacks data protection legislation,

[27] Writ Petition No. 7483 of 2020 (GM-RES-PIL).

leaving its vulnerable citizens at the mercy of data controllers and government actions. The GDPR, on the other hand, has a far broader scope and advocates a number of obligatory principles to protect EU residents' privacy rights. Article 5 establishes guidelines for the processing of personal data. The data controller must process personal data ethically, legitimately, and transparently, according to the article. It further promotes data minimization, storage limitation, purpose limitation, confidentiality, and accountability on the part of the data controller.[29] The GDPR has included health information in the "special category of personal data" as a result, stringent protections and mechanisms for the security of such data, as well as privacy and fundamental rights, are in place for the users.[30]By imposing restrictions on data collection and data sharing and also providing other privacy regulations the GDPR does not create a roadblock for contact tracing apps but rather inculcate a sense of trust in such apps by the users as both the data controller and the data subjects are well aware of their rights.[31] In the face of regulatory lacunae in India, the government must move with caution to avoid infringing on individuals' right to privacy in the zest to mitigate the menace of the pandemic.

## V. LEGALITY, OVER-ARCHING NEED AND PROPORTIONALITY

### Legality

As the pandemic began to spread rapidly the government needed to act quickly. The Indian government released various rules under the National Disaster Management Act, 2005, in an endeavour to contain the

[28] *Hindsight is 20/20: Assessing outcomes from AarogyaSetu,* INTERNET FREEDOM FOUNDATION, https://internetfreedom.in/the-past-and-future-of-aarogya-setu/ (last visited on October 3, 2021).

[29] Art. 5 GENERAL DATA PROTECTION REGULATION, Principles Relating to Processing of Personal Data.

[30] Maria Pia Sacco et al., *Digital contact tracing for the Covid-19 epidemic: a business and human rights perspective*, INTERNATIONAL BAR ASSOCIATION,https://media.business-humanrights.org/media/documents/files/documents/LPRU-Digital-contact-tracing-COVID-19-June-2020.pdf (last visited on September 26, 2021).

[31] Laura Bradford et al., *Covid-19 contract tracing apps: a stress test for privacy, the GDPR, and data protection regimes*, JOURNAL OF LAW AND THE BIOSCIENCES, (May 28, 2020),1-21.

disproportionate transmission of coronavirus, one of which was the use of contact tracking tools through its AarogyaSetu app. However, this technology was deployed through mere executive orders and lacked adequate legal backing. The data sharing protocol the government issued after introducing the app only explained in the manner the data must be collected and shared which was not enough to defend it against a constitutional challenge to its legitimacy.[32]

Considering the Disaster Management Act to be a valid legal basis for using the AarogyaSetu application is wrong, as the Act makes no mention of the government's right to limiting or infringing on citizens' right to privacy. If the government believes that it can take any decision which it considers to be reasonable in the public interest, it undermines the values of rule by and of law leading the country towards rule by the executive. The existence of specific legislation governing the use of user data in the country is a vital constitutional matter and not just a procedural quirk. If the government believes it is necessary to limit the privacy rights of people, which, as previously said, is not an absolute right, the least it can do is authorize such action through members elected to the Parliament, in conformity with the "separation of powers" tenet of the Indian Constitution.[33]

**Over-arching Need**

The second criterion is whether such a law required by the State is based on a legitimate objective. Keeping the present scenario in mind the main objective of the State is to work towards the protection of life and health of its citizens. According to the Privacy Judgment of the Hon'ble Supreme Court in a situation of an over-arching need, any State action enforcing the invasion or infringement of privacy rights of people must be free from apparent arbitrariness. No doubt the State has a legitimate aim of mitigation of the disease but making the AarogyaSetu app mandatory which has no

[32] Rahul Matthan, *The Privacy Implications of Using Technologies in a Pandemic*, JOURNAL OF THE INDIAN INSTITUTE OF SCIENCE 100 ,4 (2020).

[33] Kesavananda Bharti Sripadagalvaru & Ors. v State of Kerala & Anr., (1973) 4 SCC 225; AIR 1973 SC 1461.

legal backing suffers from arbitrariness on the part of the State. Also, in a country where almost two-thirds of the population is bereft of a smart phone, the use of such technology to achieve state goals appears to be a far-fetched dream. Thus, questions of its effectiveness arise as for the app to be successful at least 50% of the population must download and update it at regular intervals. Further, the app depends on the self-assessment data provided by the users about their health status. It is impossible to track infected persons who have not updated their positive status on the app.

A valid question to be pondered on is if the application was so effective and designed keeping in mind the over-arching presence of need of helping the citizens in these uncertain times why the application wasn't upgraded during the second wave which hit the country in the months of April and May 2021. Why wasn't the application used to help people find oxygen cylinders or hospital beds during this time? People desperately ran from post to pillar in order to arrange oxygen cylinders or hospital beds for their near and dear ones leaving the already vulnerable citizens to fend for themselves. These months saw the maximum casualties in the country with help arriving from nowhere.

Later the app was integrated with the COWIN app for vaccination management which also registered people collecting their Aadhar numbers, raising further concerns of violation of privacy. The government went a step further through its recent project creating Aadhar linked national health IDs (including beneficiary's detailed health records to be used by the government, private hospitals, and insurance firms), to build 'National Health Stack' (NHS) using the data collected through the COWIN app. Hence, strengthens the concerns of data privacy activists and also questions the fact whether there was an over-arching need for using such technologies to mitigate the pandemic or was it a foundation stone installed by the government for the collection of enormous data of its citizens for a much larger purpose other than the present situation.

**Proportionality**

Data protection was recognized by the Hon'ble Supreme Court as an indispensable part of privacy rights in the *Puttaswamy* case. While examining the proportionality principle regarding data protection one must keep in mind the following three global standards acknowledged around the world. These are:

a) Purpose limitation and Data use restriction,

b) Data minimization and

c) Storage restriction

The Purpose limitation[34] can be understood as -the state must collect data only for the purpose it has previously stated and not for any other purpose other than that. The purpose limitation principle mandates that the data collector/fiduciary must disclose the purpose for data collection and not ask for any consent that may empower the data collector with an unhindered right to collect excess data and access rights. The use limitation principle provides that once specifying the purpose of data collection the data collector must not use such data for any other purpose which also includes transfer or sharing of data for which prior consent of the user was not sorted. The ArogyaSetu app was set for the identification of persons infected by coronavirus and thereby to take necessary steps to mitigate its spread. Certainly, a purpose exists as echoed by the Data Sharing Protocol.

Secondly, the data collector/ fiduciary shall not gather more data than is required for the given purpose, according to the principle of data minimization[35].This principle keeps a check on the amount of data collected by the data collector/ fiduciary by evaluating whether the data collected is not more than that required to fulfill the purpose. Evidently, the ArogyaSetu App collects information more than that is required. Agreed that there exists a clear purpose to fight the disease, but one may wonder how information

[34] § 5, Personal Data Protection Bill, 2019: Limitation on purpose of processing of Personal Data.
[35] § 6, Personal Data Protection Bill, 2019: Limitation on collection of Personal Data.

like gender, smoking habits or profession has any correlation with the mitigation of the disease. Unlike other apps which use the decentralized approach AarogyaSetu app collects the GPS location of a device along with the Bluetooth information. To identify infected people and warn others who may have come in close proximity of such persons Bluetooth technology has proven to be more than enough. By collecting GPS location data of infected citizens, the government has opened a pandora of concerns regarding mass surveillance which may become a permanent approach in the near future.

Finally, the concept of storage limitation[36]emphasizes that after the goal for which the data was acquired has been met, the data must be removed. The data collector/ fiduciary must not retain it longer than required. To fulfill this principle the data collector/fiduciary is bound to evaluate periodically if the data once collected is required to be retained any further. The '*AarogyaSetu Data Access and Knowledge Sharing Protocol, 2020*' increased the time limit for storing data collected from 45 days to 180 days for persons uninfected with coronavirus as well as 60 days to 180 days for persons who have fallen sick due to the virus.[37] The protocol also mentioned that any person can request deletion of his/ her demographic data which may be deleted within 30 days. However, if a person does not make any such request the data will be held in the government servers whilst the protocol is in effect. Also, as per the privacy policy the data is stored in "anonymized, aggregated datasets" on the central server. The concern around anonymized datasets is that such aggregated datasets may be retained on government servers for more than the stipulated time. Such non-erasure of data contradicts the data retention principle. The policy also makes no mention of the fact that deleting the app from one's phone cancels one's registration too. A sunset clause is provided by the Knowledge Sharing Protocol, specifying that personal information of people will be erased following that time.[38] It

[36] § 9, Personal Data Protection Bill, 2019: Restriction on Retention of Personal Data.

[37] Amrita Madhukalya, *Govt issues new protocol for AarogyaSetu data collection,*HINDUSTAN TIMES, May 7, 2020, https://www.hindustantimes.com/india-news/govt-issues-new-protocol-for-aarogya-setu-data-collection/story-EgPaNkP06FDOy1VGOPtKBP.html (last visited on December 29,2021).

[38] *Supra* note 1, Sunset Clause, ¶10, at 5.

does, however, include a way to extend this duration. There exists a concern that the application may be repurposed to integrate it with other services like e-pharmacies, telemedicine, etc. as the app is exempted from this sunset clause.[39]

## VI. CONCLUSION

Among other response tools, contact tracing is the most vital response tool used globally by most administrations to manage the pandemic. Balancing both public interest and privacy protection is vital. These technologies can only succeed if the government earns the public's trust, which is plainly not true with the AarogyaSetu app at present. It is important for the government to remember a fundamental principle*: Citizens cannot be made safer by increasing their vulnerability.*

Building applications based on the notion of 'privacy by design' is one strategy to gain public trust. The principle ensures that privacy is considered a vital component while building any new technology for the people at large. Following the principle does not hinder innovations. In fact, it strengthens the trust of people in their government or any private player developing these technologies. Privacy by design is a critical facilitator for ethical and lawful innovation as well as personal data protection.

Further, as India is still in a process of formulating its data protection regulation the government needs to be transparent about the usage of the data collected and stored in its official servers. Even though NIC officials assured that the application will not be used beyond the pandemic, still it has become a foundation for the formation of health IDs for the 'National Health Stack' which means the government has no intentions of removing the data after the pandemic is over and will use the enormous data so collected for further purposes as it did withthe BHIM app which proved to be a foundation for 'Unified Payment Interface' (UPI).

---

[39] Shashidhar K. J, *AarogyaSetuApp and its many conflicts*, ORF, (June 06, 2020), https://www.orfonline.org/expert-speak/aarogya-setu-app-many-conflicts-67442/ (last visited on September 30, 2021).

One may consider the objectives of the government as laudable, but the app falls short of the bare minimum expectations of creating a balance between protecting public health on one hand and avoiding privacy violations of the citizens, even unwittingly. The impact of the application on the right to privacy needs to be legitimate, obligatory, and proportionate to its objectives. Even if the App and its design rationale were formulated in a hurry to take on an immediate threat, over time the same ought to have evolved to address genuine concerns of citizens regarding its impact on their rights. The government must recognize its flaws and work towards filling the gaps and own up its responsibility to protect the data and privacy rights in order to win back the trust of its people, as well as uphold the mandate of the Constitution of India.

# UNDERSTANDING THE DEVELOPING TECHNOLOGY OF SMART CONTRACTS AND ITS LEGAL POSITIONIN INDIA – WILL IT REPLACE A TRADITIONAL CONTRACT?

Palak Sethi*
Ajith N. Kale**

**ABSTRACT**

*The rapid development in the technology industry has provided humanity with the ability to interact, communicate, and share with others virtually on a global scale. Recent advancements in blockchain technology and decentralization gave birth to a sophisticated new technology called smart contracts. They are computer codes or automated actions that diligently facilitate validations and authentication and can be used in all industries where traditional contracts exist. The global smart contracts market is said to be reaching a market size of 345.4 million dollars by 2026 from 106.7 million at a Compound Annual Growth Rate (CAGR) of 18.1 during 2021-26.*[1] *However, many uncertain aspects need to be addressed, such as security concerns, privacy breaches, legality, etc. In this paper, we showcase a comprehensive overview of the developing technology of smart contracts. First, we present the basics of smart contracts and blockchain functions; Secondly, how smart contracts work, unique application scenarios, benefits, limitations, and finally, we describe their legal status in*

* *Student of School of law, Christ (Deemed to be University). The author can be contacted at palak.sethi@law.christuniversity.in.*
** *Student of School of law, Christ (Deemed to be University). The author can be contacted at ajith.kale@law.christuniversity.in.*
[1] *Smart Contracts Market Size to Reach USD 345.4 Million by 2026 at CAGR 18.1%*, VALUATES REPORTS, (2021), https://prn.to/3fBFDG9.

*India. This paper is aimed at providing guidance in understanding the recent advancements and fundamentals of smart contracts& Blockchain.*

***Keywords:*** SMART contracts, digital signature, blockchain, crypto currency, contract and cyber laws.

## I. SMART CONTRACT AND BLOCKCHAIN

In 1994 Nick Szabo,[2] a legal scholar and cryptographer wrote about how self-executing contracts or smart contracts could be developed through the clever use of blockchain technology, cryptography, digital signatures, and secure computation. Szabo realized that these contracts have vast potential and it could be created and executed digitally with ease.

A smart contract is nothing more than specific computer codes, or variables build onto the blockchain technology network wherein a computer, also known as nodes,[3] executes certain variables. Once the process is complete or a variable is fulfilled in the smart contract, the nodes will update the ledger instantly. Smart contracts can benefit individuals exchange fiat currencies, property, or anything of thing of monetary or perceived value in a highly transparent and conflict-free manner. This contract also cancels out the services of a middleman in the transaction. In a traditional contract, one must consult a lawyer or the government and pay a considerably higher fee to receive an important document or an agreement after a particular duration of time. One can better understand the meaning of smart contracts by understanding what exactly a blockchain is and how it functions. A blockchain is a series of blocks that are infused with information; such information is often referred to as metadata. This technique was initially addressed in 1991 by a group of researchers and cryptographers. It was first used to authenticate digital documents so that backdating and tampering

---

[2] Alex Lipton et al., *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, THE HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE (2018), https://bit.ly/3bJ9BHi.

[3] *Blockchain Nodes: How They Work (All Types Explained)*, NODES (2021), https://nodes.com/.

with them would be difficult or even impossible. This role was virtually identical to that of a Notary. However, it wasn't until Satoshi Nakamoto created Bitcoin in 2009 that this technology was completely embraced and acknowledged by the general public.

A blockchain can also be known as a distributed ledger that is entirely disclosed and are made accessible to the public. As and when some data has been recorded inside a blockchain, it becomes quite a difficult task to change it. A block in a blockchain contains three essential parts. Namely, the metadata, the hash of the block, the hash of the previous block. The data that is recorded in a particular and unique block depends on the type of blockchain i.e., a Bitcoin blockchain stores all the important details about each and every transaction that takes place in the blockchain. These transactions can be information of a sender, receivers, and amount of coins transacted. A hash in a block can be compared to an individual's fingerprint, as every person has a unique fingerprint similarly, the hash of every block has a unique code or block address. Once a block is created on the blockchain network, its hash is being calculated, and if there are any changes or discrepancies made inside a block, it will change the properties of the hash. Meaning hashes are very useful when someone wants to detect changes done on any blocks. Whenever the particulars information or parameters of the block changes, it no longer considered the same block. The third element inside each block is the hash of the previous block on the blockchain series or network, creating a unique chain sequence which is the most important and one-of-a-kind aspect of this technology.

This feature of blockchain is not very secure as technology has evolved multiple folds. The computational powers of computers are faster than ever before. This makes it so that whenever there is a change, or someone tampers with the information of the block, in theory, the blockchain must be invalid, but due to the computational capabilities, one can recalculate all the values of the preceding blocks in the blockchain. To prevent such security

issues and keep the blockchain unchanged after a value is recorded, blockchain has implemented technology of Proof-of-work.[4]

For instance, in the case of bitcoin, calculating the required and elements of proof of work and adding a new block to the blockchain network takes roughly 10 minutes. This makes tampering with the blocks more difficult since, the proof-of-work for all subsequent blocks in that blockchain must be recalculated. There exists another critical process that blockchain utilizes to secure itself, and that is by being distributed. Instead of relying on a central authority to administer the chain, blockchains rely on a peer-to-peer network that anybody may join. When someone joins the blockchain network, they receive a complete copy of the blockchain, which the node may use to ensure that everything is in working order. All the nodes in the blockchain create consensus and agree about which blocks are valid and which aren't. Blocks that have been tampered with will be rejected by other nodes in the network. Despite its flaws, blockchains are clearly quicker, cheaper, and more secured than many older systems. Major financial institutions are using blockchain for innovative solutions to sluggish and labour-intensive bureaucracy because to its inherent efficiency and security.

In an agreement or a contract, the clause, codes, or metadata embedded in a smart contract are distributed among all blockchain network members. There is no centralized authority that holds all the documents and controls the process.[5] There is also no human factor as the transaction is overseen by predefined codes and executed automatically once the parameters are complete. Smart contracts use cryptocurrencies to empower transactions with ease of use, just like Ethereum blockchain uses Ethereum (ETH) in smart contract transactions. Developers can create ETH-based smart contracts, implying that the users have to use Ethereum to sell and acquire services or digital goods. On some services, ETH is used as an intermediary coin. It can be exchanged for Bitcoin or other mainstream cryptocurrencies.

[4] *Proof-of-work (PoW),*ETHEREUM(2021), https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/.

[5] Kirill Yusov, *How Ethereum Smart Contracts Work Jelvix* (2020), https://jelvix.com/blog/ethereum-smart-contracts.

Smart contracts can be best explained with a simple example of a rental agreement wherein A rented an apartment from B, such a transaction can take place on the blockchain by making payments in cryptocurrencies,[6] A receives a receipt and a digital entry key which is given by B, and if in any case the key is not delivered within the prescribed time then the smart contract shall initiate a refund to A in cryptocurrency. Smart contract system works on the If-then[7] premise and is observed by thousands or millions of nodes on the blockchain, so early adopter of such technology can expect a faultless delivery, meaning according to the previous example, if B gives the key to A, B can be assured of the payment made by A and the same principle shall apply to A as well. Once code, parameters, or variables are inserted into smart contracts, neither party can meddle with them without the knowledge of the other, because all parties are concurrently notified and kept up to speed on what is going on. Harnessing Blockchain for American Business and Prosperity: 10 Use Cases, 10 Big Questions, 5 Solutions examines how blockchains can be utilized to tackle complicated challenges in a variety of business models and industries. It also discusses various challenges and solutions to these challenges, as well as the policies that the US government should implement to ensure that the advancement of this technology is not stifled. One of the sections of the paper attempts to debunk myths surrounding the use of blockchain technology, focusing on issues such as encouraging money laundering, identity theft, energy consumption, smart contracts, and whether blockchain will eventually replace intermediaries such as lawyers and banks. It is claimed that blockchain will not be able to replace actual people delivering services with artificial intelligence that allows consumers to transact directly with one another. These service providers will only be required to restructure their business models by using blockchain technology, such as legal firms engaging with smart contracts will be expected to know and understand coding. The paper supports the argument presented by the authors in this paper.

---

[6] Kate Ashford, *What Is Cryptocurrency?*, FORBES, (May 8, 2021), https://www.forbes.com/advisor/investing/what-is-cryptocurrency/.

[7] David Carl Wilson, *Chapter Eleven: If–Then Arguments Umn.edu* (2020), https://bit.ly/3vbbggx.

## II. UNIQUE APPLICATIONS OF SMART CONTRACTS

The creation of blockchain technology and smart contracts piqued a lot of people's interest. Soon others realized that this technology could be used for other things such as storing medical records, digital notaries, or also potentially could be used for collecting taxes. Here are some applications of blockchain and smart contracts currently used and also the future possibilities.

Several platforms that use smart contracts already exist, like Maker DAO[8] decentralized lending or the MLB's platform for buying and selling digital collectibles. The success of these platforms shows that when the issues are ironed out, smart contracts work flawlessly.The most popular use of blockchain and smart contracts are in an intuitive game known as CryptoKitties.[9] A simple game where users can exchange ETH for in-game collectibles. Another Ethereum based smart contract application, AXA flight insurance**.** The flight insurance company repeatedly tested the application of blockchain to use it efficiently in their services and make availing insurance simplified and efficient. AXA aims to solve a common problem wherein their clients often struggle to receive compensation for delayed flights. Insurance plays an undeniable crucial role in the economy to help health, property, or any risky insurance. Every aspect can be protected. Implementing smart contracts in insurance can revolutionize the insurance sector. Blockchain insurance platforms can avoid physical and digitize the records, which not only saves paper but also help in retracing the original information. Smart contracts can also benefit this industry by implementing automatic insurance approval and claims. The said parameter is completed in the contract. This prevents lossless payments, prevents scams, and provides community governance.

---

[8] MakerDAO*, An Unbiased Global Financial System*, MAKERDAO(2021), https://makerdao.com/en/.

[9] *CryptoKitties:Collect and breed digital cats!,*CRYPTOKITTIES (2021), https://www.cryptokitties.co/.

A European start-up named Authenteq[10] uses smart contracts to identify personal data left online, such as passwords, codes, usernames, fingerprints, or even contact information. Authenteq uses this information to protect its users and provides practical functionality by automatically verifying and authentication on any website.

For years innovation in medical record-keeping has been held back by the need for compliance as electronic health records can easily be tampered with without anyone knowing about it. Smart contracts in this situation can streamline the access of crucial health information for both the patients and the health care providers. Storing medical records on a blockchain allows only those who have access or viewing permission to access at any time securely. The smart contract allows authorized users to update, add additional documents to abide by the local laws and new regulations. These changes are backed up by the sophisticated blockchain network and authenticated cryptographically, making them more secure than a traditional electronic health record.

Trade settlement transactions can benefit immensely by using smart contracts as the traditional method are hindered by costly fees and risky settlement processes. In trade settlement contracts, the settlement period for the loans can be up to 20 days. The fact that this loan challenges the market's very uncertainty makes it highly unattractive cause there may be situations in which the settlement time is extended due to unforeseen circumstances and therefore result in delayed payments with high-interest rates. Smart contracts can aid in processes related to KYC and other necessary documentation at a much cheaper and efficient rate, reducing the cost of operations, settlement times, and most significant risks faced by either party.In the Land registration and owning process,[11] real estate agents go through a massive pile of documents regarding the loan structure, buyer-seller agreements, construction documents, etc. Such manual or semi-

[10] *About: Authenteq*, AUTHENTEQ (2020), https://authenteq.com/about/.
[11] *Smart Contract Applications, Limitations, and Future Outlook*, ITRANSITION (2021), https://www.itransition.com/blog/smart-contract-applications.

automated processes are cumbersome and are exposed to human errors. A smart contract can efficiently simplify this process as it can verify and validate such documents preserving time and costs. Such a contract is less prone to human errors, frauds, misappropriation, etc., and it can revolutionize the process of buying and selling real estate. However, local laws like RERA in India must validate or provide some regulations related to smart contract transactions in real estate.

Smart contracts are a simple yet highly efficient, cost-effective solution that makes voting[12] easy and secure. These smart contracts can be used for validating voter's ID and recording their votes on the blockchain network, accessible to only those concerned authorities. Once recorded, the voting data cannot be manipulated or altered within a blockchain network, resulting in an accurate and fair representation of public will.

A famous theory known as the Innovation diffusion theory, popularized by E.M. Rogers in 1962, explains how new ideas and innovations travel across cultures and are embraced. The theory aims to investigate key elements in the dissemination of innovations. They are the characteristics that cause an idea to spread and the significance of peer-to-peer interactions and peer networks.According to this theory we can speculate how smart contracts and blockchain technology can spread and be adopted in the economy and bring about a sense of security and efficiency in multiple applications.

## III. BENEFITS OF SMART CONTRACTS

Smart contracts can be popularly used as a way to replace a legal contract in many industries, which tend to be very expensive, complex, and time-consuming. There are various advantages of a smart contract. To start with, the central idea behind smart contracts is a blockchain network. It is a distributed ledger spread over several nodes. This network is used to verify and validate a transaction to execute the contract between the agreed parties. These transactions and agreements can be carried out in a blockchain

[12] *10 Use Cases of Smart Contracts*,DEVTEAM.SPACE (2020), https://bit.ly/3bJ6iQ7.

network anonymously and in a decentralized way, without any external enforcement or the legal system. There are various other advantages of this technology in a smart contract. Such contracts work on an if/then basis, so certain pre-conditions are set when a smart contract is executed. When these pre-set conditions are fulfilled, the smart contract is automatically executed.[13] This happens simultaneously for all the parties, and therefore it is quick functioning. This also makes a smart contract immutable and irreparable once the transaction is recorded. Suppose there is an error in the transaction. In that case, it cannot be altered or tampered with, and it can only be corrected by recording a new transaction, which will also be permanent. The permanent feature of a smart contract makes it traceable across the network. The data that exists is encrypted on a distributed ledger. The data, once recorded, is non-alterable and cannot be lost or deleted, thereby making it transparent and secure.[14]

When it is recorded, the data is shared across the network and is duplicated n number of times, due to which it can be quickly restored or traced back in the event of any data loss. Smart contracts do not need third parties to execute or validate the terms of an agreement. Thus, the risk of manipulation is negligible, as well as the cost to hire a third party, which can be hefty, depending on the agreement being eliminated, which results in cost savings. There are various other advantages of smart contracts, such as the accuracy of such contracts is higher than a traditional contract since it is not manual, and thus, there is less room for errors. It is automated and uses computer protocols to undertake tasks, saving hours of lengthy business processes.

## IV. LIMITATIONS OF SMART CONTRACTS

Notwithstanding the fact that smart contracts, if rightly used, can be highly efficient and secure, several limitations, as highlighted below, could easily prevent the masses from adopting this technology. The smart contract is not

[13] *Smart Contract Corporate Finance Institute*, CORPORATE FINANCE INSTITUTE, (2019), https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contract/.
[14] *10 Advantages of Using Smart Contracts - ChainTrade – Medium,* CHAIN TRADE, (2017), https://bit.ly/3hKaW4e.

free of human errors; these are codes written by humans and require algorithmic precision similar to legal drafting in the case of a contract. Bad legal drafting can lead to various problems. Similarly, coding requires precision, and thus there are high chances of errors that can prove to be very costly. Not only this, but a traditional contract is not entirely rigid. The terms of a contract are left ambiguous to be adaptable in the future, especially in a long-term contractual relationship which is not possible in a coded contact that has rather specific terms, which makes it rigid and deterministic, and making it adaptable would require making a lengthy contract hence increasing the chances for an erroneous contract. Another limitation is the assumption that all legal obligations can be expressed in code. A contractual obligation sometimes can be solely based on abstract legal concepts such as "reasonable," "fairness," and "good faith," these terms are frequently used in contract law[15].They are almost impossible to be represented as a code.

A blockchain, once executed, is immutable, and entries cannot be reversed. As much as this is an advantage, it can also be a disadvantage. A blockchain and smart contract is only as accurate as of its data. If incorrect and inaccurate data is entered, the blockchain will have no value. A faulty smart contract will be entered and executed automatically upon fulfillment of the predefined conditions in the worst-case scenario. Since it is immutable, there is no way to rectify the entry and prevent a faulty smart contract from being executed, costing both parties' huge sums. Except there is a famous "51% rule,"[16] which means if 51% of the chain agrees, they can allow rectification to be made. One might think of it as a solution, but it is mostly the other way round. 51% of the network can amount to millions or maybe even billions of nodes in a system. A change can only be made if this 51% of nodes approve of it. However, it has to be kept in mind that such an event is not impossible but

[15] Mik, E., Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, (2017),9(2), at 269–300, https://ink.library.smu.edu.sg/sol_research/2341. pp 20-21.

[16] Suominen, Kati, et al. *,10 Big Questions (and Myths) Surrounding Blockchain*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS), 2018,15; *Harnessing Blockchain for American Business and Prosperity: 10 Use Cases, 10 Big Questions, 5 Solutions*, www.jstor.org/stable/resrep22491.6.

less likely to happen. In this sense, a blockchain network is not truly secure, and it can be hacked using the same rule as mentioned above.

## V. LEGAL STATUS OF SMART CONTRACTS IN INDIA

In the past two decades, there has been a radical transformation in the field of technology. In merely ten years, the world has shifted from bulky phones to sophisticated and easy-to-use smartphones. If there is anything to learn from this pandemic, it is that the future is digital. Technology is an essential part of one's life today in every sector, from schools and colleges to jobs. Now, even the legal fraternity has used technology to bridge the gap. The transformation is much faster than one can imagine. In this paper, we have tried to understand the functioning of a smart contract as well as the pros and cons of this emerging technology, but the questions that remain largely unanswered are concerning the status of this technology in India. A smart contract is a futuristic digital technology,which means it is developing, but there is a long way ahead before it can be put to use. Another question that arises at this juncture is that, can we really legislate a technology that we can neither fully predict nor understand?

The Indian Contract Act, 1872,[17] is the prevailing law that governs the contract and its enforceability in India. It defined a contract as an agreement enforceable by law. To determine the legal status of a smart contract, we must refer to Section 10 of the said statute, which states the essential elements of a contract. For an agreement to be enforceable, there are three main elements offer, acceptance and consideration inter alia lawful object, free consent, competent parties, and not expressly void. A smart contract is similar to a traditional contract; the parties enter into a contract through offer and acceptance. In a traditional contract, money is the consideration, whereas, in a smart contract, money is replaced by cryptocurrency. The issue that arises here is concerning the admissibility of cryptocurrency as a

[17] §10, The Indian Contract Act, 1872.

[18] Amit Agarwal, *Ecommerce an ally in realisingAtmanirbhar Bharat vision,* THE ECONOMIC TIMES, (2021), https://bit.ly/3vfRzUS.

consideration. In India at present, there is no regulatory framework governing cryptocurrency and its functions, but trading in crypto is not illegal;[18] rather, any such ban would amount to a violation of Art 19(1)(g)[19] as held in the Internet and *Mobile Association of India v. Reserve Bank of India*.[20] In this case, the Hon'ble court held that cryptocurrency was capable of being recognized as valid payment for goods and services. However, it has to be noted that regulations and the standing of the government of India in this matter are uncertain.

Section 10A of the Information Technology Act, 2000[21] provides validation to a contract formed through electronic means when such a contract is formed through offer and acceptance. As a result, any contract entered into via electronic means will not be declared invalid just because it was entered into electronically. Section 5 of the Act legally recognizes a digital signature as a valid form of authentication. However, Section 35 of the Act requires that such digital signatures be obtained from certified government authorities. In the context of Blockchain, this digital signature is generated automatically. Therefore, contrary to the IT Act, the digital signature cannot be considered a valid form of authentication.

The Indian Evidence Act, 1872[22] lays down specific provisions concerning the admissibility of electronic records in Section 65B, which states that a document produced with the help of a computer will be considered a valid document. Section 85B of the Act provides that an electronic agreement would be considered valid only if such document is acknowledged through a digital signature. Section 88B of the Act presumes authenticity of such a document produced in the court unless the contrary is proved.

Therefore, a smart contract is well within the definition of a contract. The law does not limit the scope of a contract to a traditional contract or a paper

[19] INDIA CONST., Art. 19(1)(g).
[20] Internet and Mobile Association of India v. Reserve Bank of India [2020] 158 SCL 448 (SC).
[21] § 5, 10A & 35, Information Technology Act, 2000.
[22] § 65B, 85B & 88B, Indian Evidence Act,1872.

contract. It is capable of being extended to futuristic technologies such as smart contracts. Still, as far as the question of admissibility and enforceability is concerned, it is a legal grey area. For the time being, there is no regulatory framework for such futuristic technologies as smart contracts, blockchain, or cryptocurrency, and hence the implementation of such technology will be a difficult task.

## VI. CONCLUSION AND THE WAY FORWARD

The smart contract represents a universal technology that today's technologically advanced generation holds promising perspectives across multiple industries. It's already widely used in insurance, fintech, investment, real estate, and all forms of agreements that could be substituted. While these may be a few niche examples nevertheless, the brightest minds and latest technology are working hand-in-hand on making the smart contract an everyday reality. In 1995 during the apocalyptic dot-com bubble[23], the world economy observed a drastic shift towards the implementation of the internet to various aspects. Without the dot-com bubble crash, there wouldn't be any conglomerates such as Amazon, Facebook, Apple, etc. However, people didn't believe it at first; the dot-com bubble and the shift towards using the internet on a large scale provided people with the reasonable belief that the internet would be the next big thing positively impacting the economy.

Similarly, smart contracts have the potential to become the next "dotcom bubble" around the world, but the governments and regulatory authorities must take the first step. Adequate exposure must be given to blockchain technology in order for it to improve, and by bringing in a suitable regulatory framework, the governments can assist the process. At present, there is uncertainty regarding regulations concerning the latest blockchain technology. It becomes essential for both sectors, private and public, to present a unified front towards enhancement and mass adoption of smart contracts and blockchain.

[23] *What Ever Happened to the Dotcom Bubble?,* INVESTOPEDIA (2021), https://bit.ly/3hjjvmz.

# BLOCKCHAIN AND THE RIGHT TO BE FORGOTTEN

Anahida Bharadwaj*

**ABSTRACT**

*The dialogue surrounding the right to privacy, and its ancillary right to be forgotten, has gained prominence in recent times. Recent judgments passed by courts across the country, supplemented by the decisions of foreign and international forums, aid in providing the much-needed clarity on the matter – the right to privacy and ancillary rights are a fundamental right accorded to individuals under the Constitution of India as well as international conventions to which India is a party.*

*Technology harnessing data is now considered the most precious in the world, with data being compared to oil in terms of functionality in modern economies. Blockchain, one such development; is a distributed ledger which forms an immutable 'chain' as and when it receives additional data. Despite all benefits, a red flag for privacy analysts is the allegedly- permanence of information stored on the ledger. This is a violation of one's right to be forgotten.*

*Through this research piece, we will be tackling the following aspects: first, what is blockchain and attempts made by Indian authorities to incorporate the same in our day-to-day life; second, the emerging jurisprudence vis-à-*

* *Judicial Clerk and Researcher at the High Court of Delhi. The author can be contacted at anahidab@gmail.com.*

*vis the right to be forgotten and third, whether the adoption of blockchain technology can infringe upon the constitutionally-enshrined right to be forgotten.*

***Keywords:*** *Right to privacy, Blockchain technology, Constitution of India, Right to be forgotten.*

## I. INTRODUCTION

Data is referred to as the oil of the 21st century – a statement that irks economic critics and scholars. The finite quantity of oil on this planet is a crucial determinant of its price, making it virtually immune to the economic laws of diminishing marginal utility.[1] The satisfaction derived from oil consumption does not wane despite factors such as the availability of alternative, greener fuels and the cumbersome, costly process of extraction.

Data, on the other hand, is an infinite resource. By the time the author would finish typing this sentence, an incomprehensible amount of data would have been generated in her neighbourhood itself. The comparison to oil stems from the role data plays in the modern digital economy. Each unit of data produced is as, if not more, valuable than each drop of oil trapped under this planet's surface. Oil was a key element vis-à-vis functionality of innumerable sectors in traditional economies. The ever-growing importance of data and developing technologies for data-processing and collection as its basis reaffirms the claim of 'data being the new oil'.[2] The value assigned to data makes it highly susceptible to be the subject of trade, with the constitutional rights of freedom of trade[3] and freedom of speech[4] permitting data to be sold like hot cakes.

---

[1] Rashmi Rana, Ruchi Sharma and Shivani Kashyap, *Consumer's Equilibrium,* 1 IJIRT 729, 730 (2014) (discussing the law of diminishing marginal utility).

[2] Kiran Bhageshpur, *Data is the New Oil and that's a Good Thing,* FORBES, NOV. 15, 2019, https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/.

[3] INDIA CONST., art. 19, § 1, cl. g.

[4] INDIA CONST., art. 19, § 1, cl. a.

Law serves the purpose of protecting the inalienable rights of man-land, self and liberty. Data, including personal data, generated by an individual has in the recent past become an intrinsic part of one's self, and is eligible to be accorded the same protection to the aforementioned inalienable rights. Thus, the rights over data created and held by an individual would be subject not only to constitutional trade laws but also to the fundamental rights to life and personal liberty[5]. Another right under the umbrella of right to life and liberty is the right to privacy of data, including personal data. The right to privacy, as elaborated upon later, is not absolute and has a sub-set of the right to be forgotten; thereby creating a systematic anomaly of attempting to create a balance between the right to use data-harnessing technology for trade purposes and the right to one's life and liberty.

Through this research piece, we will be tackling the following aspects: *first,* what is blockchain and attempts made by Indian authorities to incorporate the same in our day-to-day life; *second,* the emerging jurisprudence vis-à-vis the right to be forgotten and *third,* whether the implementation of blockchain technology can infringe upon the constitutionally-enshrined right to be forgotten.

## II. RESEARCH METHODOLOGY

This research paper elaborates upon whether the right to be forgotten and blockchain two are mutually exclusive. Writing the paper involved extensive and exhaustive qualitative research. The author utilised several online repositories, owing to lack of access to physical resources due to the COVID-19 pandemic. To develop a basic understanding on the subject-matter, the author watched educational videos on blockchain functionality. The research was further honed through written works of several academics. Here, it is pertinent to point out that international papers provided a more comprehensive base in terms of the theoretical as well as practical applications of blockchain. Given the nascent development and adaptation of the technology in India, the research here is on the theoretical side; which

[5] INDIA CONST., art. 21.

the author believes will be a lot more comprehensive in the near future. The research aspect for the right to be forgotten was a lot easier, as there was judicial precedent to rely upon as well. The effervescent and contentious nature of data privacy jurisprudence made the formulation and potential problem-solving for this grey area daunting yet thrilling. The author, in her initial stages of research, noticed that most literature on the hypothesis made a demarcation set in stone- one cannot exercise their right to be forgotten in a blockchain network. The little privacy accorded in a blockchain network is a cause of concern and attempts should be made to reverse the demarcation made. However, further research did help the author arrive at a conclusion wherein the two fields can exist co-dependently as well as independently; as is explained later in the research piece.

## III. WHAT IS 'BLOCKCHAIN'?

Conceptualised by Satoshi Nakamoto, the identity of whom (or a group of individuals) remains unknown till date, blockchain was first popularised in 2009, when a cryptocurrency by the name of "Bitcoin" was developed by Nakamoto using blockchain.[6]

Blockchain, which applies distributed ledger technology, is considered to be the next big thing in terms of technological simplification. Blockchain technology enables users to conduct their transactions on a decentralised, peer-to-peer network. A peer-to-peer network is one where the data generated and stored by one individual is available to each and every one who is a part of the same in an equal and unbiased manner.[7] A transaction requested would be broadcast and subsequently verified by the existing nodes or "blocks" which form part of the network and then create a new block.[8]

---

[6] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system,* https://klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf ,Accessed on Dec. 30, 2021.

[7] Georgios Dimitropoulos, *The Law of Blockchain,* 95 Wash. L. Rev. 1117, 1127-1130 (2020) (discussing the development and working of blockchain).

[8] *Id.*

Under the following headers, we will attempt to learn about the working and benefits of blockchain technology:

### i.) The working of Blockchain Technology

#### a. Internet of Things

Blockchain and its similarly-placed concept of 'Big Data' form a small part of the Internet of Things ('IoT'). The IoT refers to an interlinked network of objects, where the data is sent via a tag or microchip.[9] The IoT's functionality is dependent upon linking two or more objects (whether physical or digital). The coupling of IoT with blockchain enables the creation of impermeable records of the transactions and processes conducted applying the same.[10]

Prominent examples of devices adapting this technology include smart televisions, fitness bands, virtual assistant devices and self-driving cars. The objects in the network formed can "communicate" amongst one other like living creatures- giving them the ability to disclose any and all information, including that of sensitive and personal nature. This is an alarming development from a privacy point of view. The increased usage, supplemented by uninformed usage and lack of effective updates from the company's end exposed cybersecurity vulnerabilities in the system, yet leading to a blind rise in the devices owing to the ease of task-performance provided. This necessary evil is omnipresent across technology operating using this as their base, leading cyber-security experts to sound the alarms on the implicit consent we provide to entities to collect our data.

#### b. What is a 'ledger'?

A "ledger" is a digital version of the financial transactions conducted by an individual or an entity, similar to the physical volumes maintained by

[9] Nicola Fabiano, *The Internet of Things ecosystem: the Blockchain and privacy issues: The challenge for a global privacy standard* https://ieeexplore.ieee.org/document/8008970, Accessed on Oct. 01, 2021.
[10] *Id.*

businesses. The permanence of the records is what sets this technology apart from their physical counterparts. Blockchain uses this distributed ledger technology to maintain a decentralised database, where multiple individuals can store synchronised copies of the same data.[11]. The transactions and their corresponding timestamps, conducted through blockchain are maintained in the form of blocks. These blocks or nodes are linked together like a decentralised peer-to-peer network, in a digital sequence or a "chain".[12] The data recorded in the digital ledgers is permanent and secure. The network is supported via a series of blocks, with each transaction being added to a new block. A new block is added to the sequence after solving a cryptographic puzzle.[13]

The data immutability provided by blockchain technology is done through the use of hash functions and digital signatures, which surprisingly were defined under the Information Technology Act, 2000 ('the IT Act')[14]. The definition provided in the Indian legislation has stood the test of time and can now be utilised to help draft effective legislation for blockchain as well as its subsequent usage in India.

### c. Types of Blockchain

Blockchain technology is not the infinite network it advertises to be. The technology can be used in two forms – permissioned or permission-less. Permission-less blockchain is an open network with an unlimited number of nodes in the sequence.[15] In the event a user is on a permissioned blockchain, they are working on a closed network with a limited number of blocks. Actions on a permissioned blockchain are only performed by designated nodes, creating a more secure network as opposed to open access to one's

---

[11] *Supra*note 7.

[12] Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, *Blockchain Demystified: a Technical and Legal Introduction to Distributed and Centralized Ledgers*, 25 RICH. J.L. & TECH 1, 16 (2018) (discussing the technology behind blockchain technology).

[13] *Supra* note 12.

[14] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), http://indiacode.nic.in.

[15] *Supra* note 7.

data being provided in a permission-less blockchain.[16] Blockchain technology can further be divided into public and private blockchain. A private blockchain is controlled by either an individual or a body corporate.[17] Despite the element of immutability still being rampant, permissioned and private blockchain act as a mellow roadblock to privacy violations. Though the information stored won't be readily available to the world at large, users of either form would have access to all data present and could potentially misuse the same.

### ii. Benefits of Blockchain

The socio-economic benefits of blockchain technology at this juncture of the century cannot be ignored. The key features of blockchain; which are its efficiency, transparency and increased security, form the root for its willing adaptation across the board.[18] Research conducted by IBM listed the following as the most-prominent industry-wide applications of blockchain technology:

- Streamlining supply chain management would ensure increased accountability among actors in the chain, thereby allowing speedy action in the event of a mishap;
- Increased operational facilities spread on a global level would allow faster, smoother banking operations; and
- The maintenance of a mammoth patient database that can be accessed by concerned parties would allow for more comprehensive healthcare provision.[19]

The two common contexts in which one would have heard of blockchain technology application would be smart contracts and cryptocurrency. The

[16] *Id.*
[17] *Id.*
[18] MarjoleinBusstra, *Designing for Good: Blockchain Technology and Human Rights*, 2020 INTERGOVERNMENTAL ORG. IN-houseCouns. J. 31 (2020).
[19] *Id.*

obvious benefit of smart contract usage, powered by blockchain, would be the universal availability of the content, facilitating international trade and e-commerce.[20] As mentioned above, the evolution of blockchain began with Bitcoin; the first peer-to-peer cryptocurrency.[21] Cryptocurrencies are secured by cryptography, which makes counterfeiting or double-spending the currency virtually impossible.[22] However, the decentralised nature of the currency allows it to exist outside the ambit of governmental supervision. This is a red flag for not only current cryptocurrency utilisation but also any future implementation of blockchain, where the lack of any supervision is similar to a bull in a china shop- borderline chaotic. While excessive legislation could hamper any potential well-being adoption, finding the right balance can be achieved on a hit-and-trial basis.

### a. National Level Blockchain Framework

The benefits of blockchain have been recently recognized in India as well. The Ministry of Electronics and Information Technology (MeitY) released the Draft National Strategy on Blockchain in January 2021, which recommended the creation of a National Level Blockchain Framework (NLBF).[23] The NLBF has the potential to allow shared, stable infrastructure and enable cross-domain application development. The stable infrastructure, according to MeitY, has to be developed keeping in mind the shortcomings on the Indian front. The rise of e-governance schemes, such as Digilocker (storage of soft copies of official government-issued identification cards), National Faceless Assessment Centre (conduct of scrutiny and assessment of income tax returns filed by an individual for any assessment year) and the

---

[20] Laya Aminizadeh, *The Blockchain Technology and Legal Challenges,* 2020 REV. FAC. DREPT ORADEA 139, 140-142 (2020) (discussing the benefits of blockchain as well as the possible legal roadblocks the technology faces).

[21] IlkerKoksal, *The benefits of Applying Blockchain Technology in any Industry,*FORBES, Oct. 23, 2019, https://www.forbes.com/sites/ilkerkoksal/2019/10/23/the-benefits-of-applying-blockchain-technology-in-any-industry/?sh=3723f86a49a5 .

[22] *Id.*

[23] Aashish Aryan, *IT Min suggests blockchain use in public projects,* THE INDIAN EXPRESS, Feb. 5, 2021, https://indianexpress.com/article/business/it-min-suggests-blockchain-use-in-public-projects-7175027/.

recent faceless method adopted by Regional Transport Offices in Delhi, to name a few; stand to benefit from the effective utilisation of the NLBF.

## IV. RIGHT TO BE FORGOTTEN

Uppaluri, in a working paper, observed that data protection laws legislate the treatment meted to data, including sensitive and personal data, at different stages of processing the same.[24] In the same paper, the following were held to be the cornerstones of any data protection law:

- Emphasis on prior and informed consent;
- Statement of purpose for which the data is being collected;
- Reasonable measures are undertaken to ensure data privacy; and
- Accountability on part of the data collector and processor.[25]

The "right to be forgotten" principles stem from a concept in international law known as "*Droit à l'oubli",* which is French for *"right to oblivion"*. The principle was applicable in criminal law, wherein under exceptional circumstances a convict who had served their sentence and wished to have their name redacted or removed from criminal records could do so.[26] In the case of *Melvin v Reidi*[27]*,* the right to be forgotten was first recognized as part of one's right to privacy.[28]

The advent and subsequent advancements made in technology have inadvertently made data retention on pockets, offline as well as online, permanent. This digital footprint is a matter of imminent concern, as it can

---

[24] UjwalaUppaluri, *Digital Memory & Informational Privacy: Reflecting on the EU's 'Right to be Forgotten'*,<https://drive.google.com/file/d/0BwY1OLu_H1ICRTRaWEtTOVFFVlU/view?resourcekey=0-SPP5S1SwIJm9V2AnEl6Mhw>, Accessed on Oct. 02, 2021.

[25] *Supra* note 20.

[26] Tejashree J, *The Need for the Right to be Forgotten in India,* 5 RGNUL FMLR 107, 109 (2018) (discussing the origins of the right to be forgotten and issue of concern in the digital space).

[27] 112 Cal. App. 285, 297 P. 91 (1931).

[28] Shreya Bansal & Deboleena Dutta, *Right to be Forgotten: A critical and comparative analysis,* 5 RGNUL FMLR 86, 91 (2018) (discussing the emergence of the right to be forgotten in the United States).

infringe upon one's fundamental right to be forgotten.[29] One could argue that the right to privacy is an antonym to the complete unavailability of information in the public domain[30]. This proposition may be correct; however, it does not mean that a data principal does not have the power to ensure that certain sensitive information is not readily available for the world to see. A further sub-set of the right to erasure, the right to be forgotten puts the ball in a person's court and not an algorithm's, concerning what information is deemed appropriate to be displayed on a global scale.[31] To prevent the gross disparity between large technology companies and governments on the one hand and the individual who permanently stored data on the other, it is imperative to hand the reigns with the data principal. The right to be forgotten, in its allegedly nascent stages of evolution, can be understood by a comprehensive comparison under the following headers:

### (i) Indian perspective

### a. The Constitution of India

The right to privacy; and subsequently the right to be forgotten, is neither explicitly granted in the Constitution, nor is it explicitly acknowledged in any international convention. Thus, the directive principle of the State to respect international treaties and obligations would not apply.[32]

In *Justice (Retd.) K.S. Puttaswamy*[33], the Hon'ble Supreme Court of India held the right to privacy to be a part and parcel of one's right to life and liberty[34]. A notable inclusion under the right to privacy was by Hon'ble Mr. Justice SK Kaul, wherein he held that the right to privacy encompasses the liberty granted to an individual to obliterate their existence.[35] This simple

[29] *Supra* note 21.
[30] Charles Fried, *Privacy,* 77 YALE LR 475, 482 (1968) (discussing the meaning of 'right to privacy').
[31] *Supra* note 20.
[32] INDIA CONST., art. 51.
[33] Justice (Retd.) K.S. Puttaswamy v Union of India, (2018) 1 SCC 809 (India).
[34] *Id.*
[35] *Id.*

observation by Justice SK Kaul permitted the right to be forgotten to be accorded the same protection under the umbrella right to privacy. This right to be forgotten was an all-encompassing right available not just in the digital space but also in the physical one. The right to be forgotten, as envisaged by Justice SK Kaul, is subject to other fundamental rights like the freedom of speech and expression[36] as well as information of public interest, research etc.[37]

The growing awareness of this inherent fundamental right has opened a floodgate of well-intentioned litigation before the Indian judiciary. In *Jorawar Singh Mundy*[38], a Single Bench in the High Court of Delhi ordered Google India and Google LLC to take down an impugned judgement from their search results. Indian Kanoon and vLex.in, noted Indian legal search engines, were also directed to take down the judgement which was causing personal and professional inconvenience to the petitioner. The petitioner in the case was an American citizen of Indian origin, who was acquitted of charges levelled against him under Indian narcotics laws. Ashutosh Kaushik, an Indian reality television star, has also approached the same forum praying for the erasure of content on the internet; citing the same as his fundamental right to be forgotten. The petition filed by Kaushik states psychological pain caused due to the permanent records of his past diminutive acts.[39] The balance, however, is not always in favour of the right to be forgotten. In *Dharamraj Dave*[40], the petitioner's plea for redaction of his name from a non-reportable judgement online despite his acquittal was not held to amount to a flagrant violation of one's right to be forgotten under Article 21 of the Constitution. A similar decision was passed recently by the High Court of Madras in *Karthick Theodore*[41].

---

[36] *Supra* note 4.
[37] *Supra* note 33.
[38] Jorawar Singh Mundy v Union of India, 2021 SCC OnLine Del 2306 (India).
[39] Ashutosh Kaushik v Union of India &Ors., WP(C) 6790/2021 (India).
[40] Dharamraj Dave v State of Gujarat, 2015 SCC OnLineGuj (2019) (India).
[41] Karthick Theodore v Madras High Court, 2021 SCC Online Mad 2755 (India).

### b. Personal Data Protection Bill, 2019

As of this moment, there is not an exclusive data privacy law in India. A germane question was raised in an article in *The Wire*- whether the right to be forgotten would stem from solely the source or from the root in the absence of a data protection law.[42] Moreover, the lack of an explicit law governing the subject requires one to seek legal redressal under other statutes, which may not necessarily address the concern one is facing. The closest India came to a data protection law is the Personal Data Protection Bill, 2019 ('PDP Bill')[43]. In its present form, Clause 20 of the PDP Bill grants the right to be forgotten as an intrinsic right to a data principal. The clause states that the collection of data contrary to the provisions of the PDP Bill or any other law at the time in force is a ground to seek data removal. Sub-clause (2) states that this right to be forgotten can be exercised upon the passage of an order by the Adjudicating Officer, who has to keep factors such as the sensitivity of the personal data, the scale of disclosure and the level at which this data can be accessed as well as the role of the data principal in public life in mind.

- **Justice BN Srikrishna Committee Report**

The BK Srikrishna Committee constituted to formulate a data privacy legislation in India, had commented upon the dynamic nature of the field which could not be governed by law set in stone ('the Report').[44] The Report had acknowledged a data principal's right to be forgotten, wherein the data principal would have a legal right to seek restriction or removal of their data either upon the personal data serving its purpose or due to withdrawal of consent on the data principal's part.

---

[42] Sohini Chatterjee, *In India's Right to Privacy, a glimpse of the Right to be Forgotten,* THE WIRE, Aug. 28, 2017, https://thewire.in/law/right-to-privacy-a-glimpse-of-a-right-to-be-forgotten.

[43] The Personal Data Protection Bill, 2019, Gazette of India, pt. II §2 (Dec. 5, 2019).

[44] M Sridhar Acharyulu, *When it isn't right to forget,* THE INDIAN EXPRESS, Sept. 14, 2018, https://indianexpress.com/article/opinion/columns/personal-data-protection-bill-2018-justice-bn srikrishna-committee-5355284/.

### c. The Indian Penal Code, 1860

Section 228A of the Indian Penal Code, 1860[45] as well as Section 23 of the Protection of Children from Sexual Offences Act, 2012[46] mandate the masking of the names of sexual assault victims. Recently, several celebrities came under fire for violating the aforesaid provision.[47] The presence of a mineral in nature does not vitiate its existence before discovery. The status of "emerging field" granted to the right to be forgotten in India is an incorrect proposition, as decisions of the Apex Court, as well as High Courts in India, have dealt with the same in a pre-*Puttaswamy* world, in not so many words. The Hon'ble Supreme Court in *Putta Raja*[48] as well as *R. Raja Gopal*[49] held that the non-disclosure of names of sexual assault victims would prevent alleged stigma and ostracism that a victim could face in society. The same has been upheld in *Shri Vasunathan*[50] and in *Nipun Saxena*.[51]

### d. The Information Technology Act, 2000

The IT Act provides *"legal recognition for transactions carried out employing electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce."*[52] Section 43A of the IT Act is a proactive section, under which if a body corporate responsible for processing or dealing with sensitive personal data is negligent in accordance with reasonable security measures to maintain privacy, the same is liable to pay compensation to such persons. Despite the provision defining "*body corporate*" and "*reasonable security practices and procedures"*, putting the onus of defining what would amount to sensitive personal data solely on the Central Government and professional bodies is a

---

[45] § 228A, PEN. CODE.

[46] Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012, INDIA CODE (2012), http://indiacode.nic.in .

[47] *Case Against Farhan, Salman, Akshay For Revealing Rape Victim's Identity: Report*, THE QUINT, Sept. 07, 2021, https://www.thequint.com/entertainment/celebrities/case-against-farhan-akhtar-salman-khan-akshay-kumar-rakul-preet-singh-hyderabad-vet-rape-murder.

[48] State of Karnataka v Putta Raja, (2004) 1 SCC 475 (India).

[49] R. Raja Gopal v State of Tamil Nadu, (1994) 6 SCC 632 (India).

[50] Shri Vasunathan v The Registrar General, 2017 SCC OnLine Kar 424 (India).

[51] Nipun Saxena v Union of India, (2019) 2 SCC 703 (India).

[52] *Supra* note 12.

challenging task that ought to be taken upon with a malleable meaning to prevent redundancy.

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[53] ('IT Rules 2011') were notified to ensure that a body corporate would implement reasonable security practices to ensure effective management and handling of the same. Upon collecting sensitive personal data, Rule 5(1) of the IT Rules 2011 requires prior written consent of a data subject and information like the nature and purpose collection of sensitive personal data to be informed. Rule 5(3) of the IT Rules 2011 grants the right to correction and erasure to the data subject, placing an optional obligation upon the body corporate to stop the provision of the goods or services for which purpose the sensitive personal data was collected. This obligation is specified under Rules 5(6) as well as 5(7) of the IT Rules 2011.

Till such time the PDP Bill, 2019 becomes legislation; the IT Rules 2011 are akin to a band-aid fixing a gaping wound. It is settled law that procedural law cannot override substantive law[54] and the mere presence of procedural law solving the purpose cannot be reason enough to not enact legislation to allow effective exercise of one's fundamental human right.

- **The Information Technology (Intermediary Guidelines and Digital Code of Ethics) Rules, 2021**

The Information Technology (Intermediary Guidelines and Digital Code of Ethics) Rules, 2021[55] ('IT Rules 2021'), which were notified in February 2021,

[53] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, 313 Gen. S. R. & O. (India).

[54] Shree Vijay Cotton & Oil Mills Ltd. v State of Gujarat, (1991) 1 SCC 262 (India).

[55] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 139 Gen. S. R. & O. (India).

mandate the appointment of a Grievance Officer. Under Rule 3 of the IT Rules 2021, a social media intermediary has to prominently display the name and contact details of said Grievance Officer as well as the grievance-redressal mechanism undertaken by the intermediary. A Grievance Officer's role includes acknowledgement of a complaint within 24 hours of receipt and its speedy disposal within 15 days; as well as the acknowledgement of any order, notice or direction issued either by a Court of law or a Government agency. A complainant has a right to approach a Grievance Officer if any content shared on a platform results in non-consensual exposure, implying that the right to privacy and to be forgotten remains intact.

### (ii) International perspective

#### a. Judicial Decisions

A landmark decision by the Court of Justice of the European Union ('CJEU') in 2014 guaranteed the right to be forgotten to European citizens.[56] It was the case of the complainant that this continuous display of personal data (details of an auction notice for the complainant's home even after resolution of the proceedings) vis-à-vis his residence and sought to exercise his right to erasure.

The CJEU held that in the event of any discrepancy or concern, any individual has the right to approach the search engine operator (in this case, Google LLC and Google Spain) for a takedown. The failure to do so would give a user the *locus standi* to approach Courts, seeking directions for the same.

#### b. Legislations

Two international conventions which are the basis of human rights legislations globally- the Universal Declaration of Human Rights ('UDHR') as well as the International Covenant on Civil and Political Rights ('ICCPR'),

[56] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, C-131/12.

grant privacy the status of a fundamental human right. Article 12 of the UDHR[57] and Article 17 of the ICCPR[58] accord protection to an individual from arbitrary interference with one's right to privacy.

The right to be forgotten is a crucial component of the General Data Protection Regulation[59] ('GDPR')- the European Union's premier data protection regulation. Article 17 of the GDPR expands and implements the right to erasure to each citizen of the European Union. The right to be forgotten is incorporated under Article 17(2) of the GDPR. The procedure for data erasure by a controller is not prescribed under the GDPR but commonly applied methods include physical erasure of the data or the usage of software for the same. The right to be forgotten is not an absolute right. It would not apply to data that was retrospectively processed.[60] Article 19 of the GDPR imposes an obligation upon a data controller to do "*what is technically feasible and does not require a disproportionate effort.*"

## V. BLOCKCHAIN AND THE RIGHT TO BE FORGOTTEN

Roger Clarke had divided the concept of 'privacy' into a multi-dimensional one, relating the concept vis-à-vis four categories: person, behaviour, data and communication.[61] Clarke's works make it abundantly clear that privacy is not synonymous to data protection nor can the same glove fit all. However, the right to be forgotten principles would apply the most extensively to what Clarke called "information privacy"- the closely-linked aspects of privacy of personal communications as well as personal data.[62]

---

[57] Universal Declaration of Human Rights, Dec. 8, 1948 G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948).

[58] International Covenant on Civil and Political Rights, Dec. 16, 1966 999 U.N.T.S. 171; S. Exec. Doc. E, 95-2 (1978); S. Treaty Doc. 95-20; 6 I.L.M. 368 (1967).

[59] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679.

[60] Shraddha Kulhari, BUILDING-BLOCKS OF A DATA PROTECTION REVOLUTION: THE UNEASY CASE FOR BLOCKCHAIN TECHNOLOGY TO SECURE PRIVACY AND IDENTITY, 23-48 (2018).

[61] *Id.*

[62] Roger Clarke, *Data Surveillance: Theory, Practice & Policy,* http://www.rogerclarke.com/DV/PhD.html, Accessed on Oct. 10, 2021.

Blockchain, and its applications, present a necessary evil- the non-modifiable timestamp assigned to the data being subject to permanence. On paper, the conceptual application of blockchain and the right to be forgotten do not offer a symbiotic relationship. There is no regulation to look into the usage of one's personal as well as non-personal data in the blockchain. This solid division between the two concepts also gives rise to the following concerns:

### I) Absence of Data Controller/Processor

Data privacy laws assign roles and responsibilities to various parties involved. The data processor or controller have to ensure ethical as well as legal processing and storage of a data principal's personal data with which they are entrusted. The magnitude of responsibility assigned to a data controller makes it imperative to know who they are, which is where the problem arises in blockchain usage. The decentralized architecture employed in a blockchain network effectively makes every user a data processor within the meaning of data privacy laws.[63] The technology also enables a copy of the data to be created on every device that is connected, which makes the identification of a central administrator virtually impossible.[64] In the context of the GDPR being applicable, the entity or individual responsible for running the blockchain network would not qualify as a data controller, the users of the blockchain network would.[65] It would be unfair to expect an ordinary user to take measures to help another user exercise their right to be forgotten, when they themselves might not fully understand the procedure. The need for an administrator identification would only arise in a private blockchain, making public blockchain even more susceptible to privacy apprehensions.

---

[63] Patrick Van Eecke& Anne-Gabrielle Haie, *Blockchain and the GDPR: The EU Blockchain Observatory Report*, 4 EUR. DATA PROT. L. REV. 531, 532-534 (2018) (discussing the roadblocks to coherent implementation of the GDPR with blockchain technology).

[64] Matthias Berberich& Malgorzata Steiner, *Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers*, 2 EUR. DATA PROT. L. REV. 422, 424 (2016). (discussing issues with determining the administrator of blockchain network).

[65] *Supra* note 60.

### ii) Territorial Jurisdiction

The data stored on blockchain need not be quarantined solely within the territorial jurisdiction of a nation, making the cross-border transfer of personal and non-personal data effortless.[66] In the absence of an international convention governing data privacy (the GDPR is applicable to member states of the European Union, other than that body corporates and individuals are governed by national laws), it is cumbersome to ascertain which State's laws would apply- the country where the blockchain originated from, the country where the user seeks to exercise their right to be forgotten or the countries where the users are based?

It is contended that the immutability and permanence offered by blockchain ought to be kept the same if it comes at the cost of functionality which would ensure data privacy.[67] Recent studies and proposals by academics in the field have shown that it is possible to take proactive action to ensure that one's right to privacy, and by extension their right to erasure or to be forgotten, can be exercised albeit extra measures. Per the existing blockchain norms, a block of information can be subject to deletion only if 51% of blockchain users reach a consensus.[68] The exercise of the right to be forgotten is not as easy as it sounds, as the same would require access to a permissioned blockchain with a few nodes. However, there are individuals and researchers who are actively looking into the creation of a symbiotic relationship between the simultaneous exercise of one's right to be forgotten and convenient yet impermeable technology. Srivastava and Garg, in an article in the *Economic and Political Weekly,* had recommended the creation of a new block after each block in the network to rebut the data stored in the first block, as it is functionally impossible to ensure efficacious erasure of data on a blockchain network.[69] The data could be entered into the network via an

[66] *Supra* note 19.
[67] *Supra* note 60.
[68] Ashit Kumar Srivastava & Deval Garg, *Reconciling Blockchain and Data Protection Regimes,* 56 EPW 23, 25-26 (2021) (discussing the 51% rule in a blockchain network and recommendations to enable the right to be forgotten).
[69] *Id.*

external link, allowing access to the data by jumping through another loop.[70] In 2018, a team at the University of New South Wales in Australia announced that they had been working on a process where data removal from a blockchain without harming the latter's consistency would be possible. Referred to as "Memory Optimized Flexible Blockchain", the team's peer-reviewed publication discusses a network wherein the data is temporarily stored and deletion is not a hundred percent on the MOFB, as a small trace remains as probable evidence in a future dispute.[71] The development of such forward-thinking technology ensures that the ball is in the court of the data principal, as discussed earlier. As evidenced by the aforementioned developments, the creation of a data-secure blockchain is not the mammoth task the general public is made to believe. Small steps towards a balanced approach will lead to a giant leap for mankind.

The provisions of Article 19 of the GDPR, coupled with limitations such as solely prospective application of the right to be forgotten, can help data controllers and processors strike an equitable balance between applying useful technology and ensuring a constitutionally guaranteed right. What works on the Indian front is the lack of specific legislation governing both blockchain as well as data privacy. Despite both being governed by different legs of the IT Act and its Rules, we have been granted a new lease to ensure that the law we create can strike a balance between the use of the technology as well as one's fundamental rights.

## VI. CONCLUSION

In *Subhranshu Rout*[72]*,* the High Court of Orissa acknowledged the right to be forgotten and the incongruities that arise in the absence of exclusive

---

[70] Gianluigi Maria Riva, *What Happens in Blockchain Stays in Blockchain: A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights,* <https://www.frontiersin.org/articles/10.3389/fbloc.2020.00036/full>. Accessed on Oct. 05, 2021.

[71] Ali Dorri, Salil S. Kanhere& Raja Jurdak, *MOF-BC: A memory optimized and flexible blockchain for large scale networks,* 92 FGCS 357, 370 (discussing the purpose and functioning of the MOFB).

[72] Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878 (India).

legislation. The absence of the legislation creates a systematic vacuum in the exercise of constitutional power and the limit to which it can be exercised. It is pertinent to note that this is not the end of the road in terms of technological developments. With each passing day, we are one step closer to the next big thing- be it in terms of a new application of blockchain or "the next big thing", and another human right it could encroach upon. Thus, it is almost imperative to pass some version of legislation or even guidelines, which can act as aids till such time we are minimally equipped. In the absence of a data protection regime, body corporates or entities controlling blockchain are not bound to ensure an individual's right to be forgotten is exercised in *toto*. Given the effervescent nature of data privacy jurisprudence, any enactment would have to fulfil the almost impossible task of considering present as well as future situations which would require legislation. The IT Act, taking into account hash functions and digital signatures is a good example. Blockchain and the right to privacy, with it the right to be forgotten, at the time being appear to be mutually exclusive in certain circumstances. A complete ban on blockchain can infringe upon a body corporate's freedom to carry on any business or trade[73] read with their freedom of trade, commerce and intercourse[74], the former of which is also a fundamental right under the Constitution of India. It can only be hoped that developers of this disruptive technology work out a system that guarantees one the right to privacy, while at the same time the right to be forgotten is not sought excessively or unreasonably. Until such time nothing is set in stone, we can continue to operate on a situational-basis with well-intended methods to balance rights of both parties.

[73] *Supra* note 3.
[74] INDIA CONST., art 301.

# INFORMATION AND COMMUNICATION TECHNOLOGY IN INDIAN JUDICIARY – STEPPING DIGITALIZATION

*Benerji Meghavaram**

**ABSTRACT**

*Intellectual Property Rights (IPRs) are the rights conferred to an individual/owner for her/his ideas, creation and a right given to a person who is an inventor or creator of such property to gain benefits from their creative work/knowledge, gives protection and right to the person who is the creator or inventor of such property. National IPR Policy of India recognised the need to bring the rights under one roof for the brighter future of IPRs.*

*Apropos to the ease of doing business, the Indian Legislature enacted Commercial Courts Act, 2015 with an objective to streamline and process commercial lawsuits, including IP disputes. This enactment has given a separate treatment to commercial cases, as per 2 (c) (xvii) of the which include cases relating to intellectual property rights associated with registered and unregistered trademarks, copyright, patent, design, geographical indications, domain names and semiconductor integrated circuits. The article an overview of the commercial courts dealing with intellectual property rights in India.*

***Keywords**: Intellectual Property Rights, Commercial Courts, Ease of Doing Business.*

---

* *PhD Scholar, ICFAI Foundation for Higher Education, ICFAI LAW SCHOOL, Hyderabad (a deemed to be University). The author can be contacted at benerjim@gmail.com.*

## I. INTRODUCTION

The continuous efforts of mankind since ancient times helped in advancement of technology and transportation which is a major milestone for globalization. This paved way for massive increase in trade and commerce worldwide. With the increase in integration and interaction among different nations, people, culture and organization globally, resulted in economic growth. Apart from growth in trade and business in the process of globalization new challenges came up worldwide demanding advancement of judicial system to make justice more transparent, accessible and effective. In top economies worldwide the use of new technology is not new but still there is a need for advancement in the judicial system.

The two words information and communication which are interlinked form the term Information and Communication Technology (ICT). The process of integrating knowledge i.e., telecommunications, computers and all required software, storage of data which enable user to access, transmit and manipulate information.

Information and communication technology (ICT) is a major dimension and can be treated as a backbone in the process of globalization. The new technology and high rate of innovation across the globe is an impact of ICT. Developments in Information and communication technology is a path for globalization and the advancement of ICT i.e, sharing of knowledge and information have transformed the process of globalization by making the economies closer. Claude Elwood Shannon is the father of information and communication technology.

With the advent of digitization there is a change in work culture in organizations, education, travel, health, shops and in every pace of life. The traditional method in storage of information such as papers, books, files, photos transformed to computer storage i.e, the binary codes ones and zeros. It increased the way of communication, elimination of paper process, data is secured, minimized the cost and time with quick process and procedure

## II. INDIAN SCENARIO

*In the digital era, it is difficult to think of any event in our daily life without Information and Communication Technology (ICT).* Our colleges, classrooms and Courts are no exceptions. The implementation of ICT tools in various sectors is a milestone to economic development of the country. Modern technology brought development in various fields with improved efficiency, save money and time management. Implementation of technology in the judicial system ensures better resolution of disputes and efficient administration. Some studies say over 4 crore cases remain pending in various courts in the country. Most cases run for many years. The Indian judicial system felt the need to improve the administration of Court activities and introduced new technology.

Judicial system is actively working to bring changes to its old administrative setup and initiative has been taken to bring better innovative results. Technology was brought in to the judiciary way back in the 90's but it was limited. As we are in a digital era the need for technology has gained more importance in every phase of life. Technology was introduced in every sector which is the need of the hour.

The covid-19 pandemic brought many challenges demanding a new way or a new innovative technology to cope up with the situation. The judiciary too came with new innovative works such as virtual hearings through video conference and encouraged to apply new technology in courts with an aim to ensure effective remedy related to emergency matters.

An idea to take accordant Information and Communication Technology (ICT) in Indian judiciary took firm condition with the constitution of the E-Committee by the Government of India in 2004. In the year 2005 E-Committee recommended the National Policy and Action Plan to present ICT in the Indian Judiciary . ICT brought more opportunities and along with it also thrown challenges to the developing nations. India is no exception. In the year 1990 Indian government brought major economic reforms with an

objective to make the economy of India to reach global standards. After the reforms the economy became more vibrant by growth in GDP with the contribution of technology which is a key factor in growth and development. The e-Courts Integrated Mission Mode project, the e-Courts Services application, zero pendency courts, and many fresh initiatives are taken to discover solution to the problem. Courts faced major challenges during the pandemic. Digitization played a key role to overcome the issues faced by the Courts during covid-19 crises. At present the government is stepping towards digitization to make India a knowledge hub and to bring technology closer to its citizens with improved online infrastructure and connectivity.

## III. OBJECTIVES OF THE STUDY:

1. To Study identify the technology closer to its stake holders with improved online infrastructure and connectivity.

2. To identify the benefits in Implementation of ICT in the Indian judiciary.

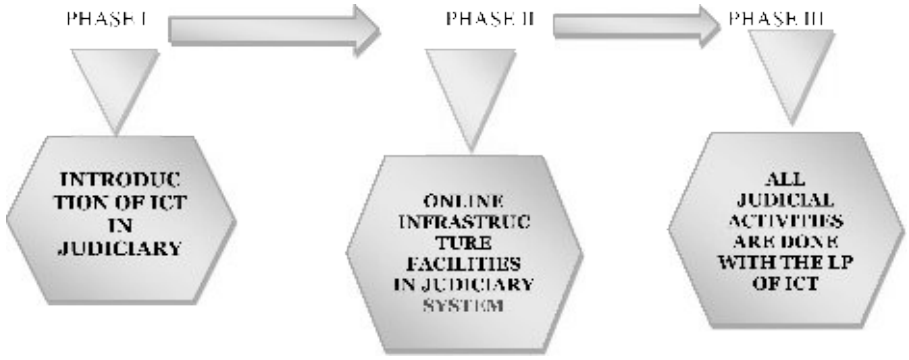
3. To critically examine the challenges faced for effective implementation of ICT in Indian Judiciary.

## IV. RESEARCH METHODOLOGY

The study is conducted basing on secondary data and data is collected from various sources particularly parliament of India reports, Statutes, journals, newspapers, websites and published articles relating to this particular topic.

## V. E-COURTS IN INDIA

An idea to carry accordant ICT in Indian judiciary took firm condition with the constitution of the E-Committee by the Government of India in 2004. In the year 2005 E-Committee recommended the National Policy and Action Plan to present ICT in the Indian Judiciary and the concept of E-Courts brought under this operation.




Phase-I: This is the initial step towards digitization of courts in the country. In the year 2007, basic case related services were provided to litigants and lawyers in courts across the country. More number of courts-initiated websites, AN, installation of hardware, CIS to provide better services to stakeholders. Training is conducted by technology experts to all court staff and judicial officers for better use of technology to improve the work efficiency of the judiciary. The phase I project ended on March 2015 with new hope towards phase II.[1]

Phase II: In the year 2014 the 2nd phase of the E-Courts mission got approval from the Hon'ble Chief justice of India and the government sanctioned in 2015. In this phase the government headed towards establishment of better technology in courtrooms. The uncovered courts in phase I are covered in phase-II with better hardware and LAN facilities.

Online infrastructure facilities provide cloud computing which is cost effective and digitization of court complexes to provide better services to the stakeholders. The court complexes are connected with jails to conduct video conferences which made the judiciary to overcome few difficulties in specific cases. In phase II core-periphery model software was developed as per the requirement of courts. The expertise of judicial officers and re-engineering

[1] *The e-Committee, Information and Communication Technology in Indian Judiciary, SUPREME COURT OF INDIA, ecommitteesci.gov.in/project/brief-overview-of-e-courts-project.*

process in phase II render knowledge management such as integrated library management and e-libraries. The information related to the cases will be provided in the court website in local languages, messages, emails, SMS, mobiles are used to share information within the court system. NJDG will be more advanced to provide better information to stakeholders.

Phase III: The vision of phase III is a draft document which tries to adopt an ecosystem concept where the process of interaction of systems involves. Digital case management systems, e-filing, digital hearings etc., are the developments initiated in this stage. To make phase III successful it is necessary to bring data protection laws.

The Indian judiciary consists of nearly fifteen thousand courts with 2500 court complexes. The ICT proposal was initiated at three phases in Indian judiciary under the E-courts MMP project for a period of five years with an aim to implement automated decision support systems in seven hundred courts in cities like Chennai Mumbai and Kolkata, nine hundred courts across states and union territories and 13,000 district courts and subordinate courts across the country[2].

In the year 2015, on July 1, the government initiated Digital India campaign with an aim to transform India as digitally empowered in the field of technology so the government services are made available to the citizens electronically with better internet connectivity in rural areas too. The digital India objective will surely enhance the economic growth of the country. Online infrastructure facilities and better internet connectivity will boost the growth in various sectors which throw a positive impact in the development of the nation[3].

Pending cases in various courts across the country is an overburden on the Indian judiciary. To reduce the burden the government felt the need to bring

---

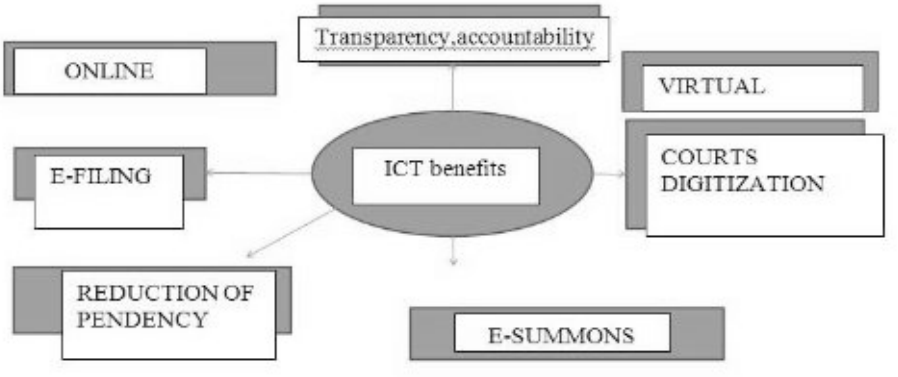
[2] *Ministry of Electronics & Information Technology, GOVERNMENT OF INDIA, www.meity.gov.in/about-meity/functions-of-meity.*

[3] *5 Years Of Digital India – How Far Have We Come? (2020), https://www.dqindia.com/5-years-of-digital-india-how-far-have-we-come/.*

reforms in the judiciary system. To make the judicial process more cost-effective and transparent the government implemented ICT in the judicial system.

Digitization of court proceedings gained more value due to covid-19 situation. The judiciary opted e-filings for crucial matters and conducted proceedings through video conferencing mode. The e-courts project came up with an objective to use ICT at different phase's i.e., to initiate single stop filing centres, e-payment gateways, and e-filing performance. The objective of the project is appreciable but the aim and objective of the project can be achieved only when there is proper knowledge and awareness among judges, lawyers, public and the people involved and connected with the courts.

## VI. BENEFITS IN IMPLEMENTATION OF ICT IN THE INDIAN JUDICIARY




**Reduce the rate in pending cases**: Digitization of court rooms helped to reduce the pending cases. Wi-Fi connection and computerization of courts by the government boosted the justice delivery system in Indian courts. Even during the covid-19 pandemic the judiciary came up with e-filing and video conferencing for urgent cases in order to provide justice in time. The up gradation of ICT in the courtrooms is a boon to the judicial system which benefited to cut down pending cases to some extent.

**Transparency and Accountability**: The use of ICT in judiciary is an ample benefit to the stakeholders. The litigants can access to the information with more transparency, and accountability of judicial administration can be improved where there is no possibility to mislead any data or information. The confidentiality of proceedings can be maintained in proper manner as per the Court structure.

**E-filing of cases**: Usually the cases are filed physically but after initiation of ICT with an aim to upgrade judicial infrastructure the e-filing process was introduced in various courts across the country. This is the best mode of convenience to the stakeholders with significant reduction in consumption of paper. The process of sharing and accessing digital documents online is time saving and cost effective.

**Digitization of Court**: Digitization of court records is a major reform brought in the judiciary system. The information and documents related to the courts are stored into a database which is easy to access. Paperless process, recording of court proceedings, video conferencing, court live proceedings can be viewed by the authorized people from the website of the court.

**E-Summons**: The government has taken major steps to merge technology in the judicial system. This initiation benefited the judiciary to provide justice to the litigants during the covid-19 pandemic. The e-service of summons is one among the up gradation of technology in the judicial process. After the initiation of ICT courtrooms started service of summons through emails, WhatsApp and e-messages which is time saving and cost effective.

**Online Proceedings**: Online court proceedings came as a boon to the judiciary. Selected Court cases which are urgent are done through video conferences during the pandemic conditions when there is strict guideline of physical distancing. Different modes of electronic instrumentation are used to conduct court proceedings which helped to overcome the delay in disposal of cases.

**Virtual Courts:** The concept of virtual courts was first given by the professor Federick I lederer, working as the Director in US Center for Legal and Court Technology. He defined the structure of courtroom as information hub and a system of management and center for information exchange. Hence, virtual Courtrooms are possible with high technology which is helpful to lawyers and judges.

In the year 1997, professor Lederer predicted that information and communication technology will play a significant role in the near future. The use of technology in every facet of human life will modify the standard of living and improve the efficiency of the courtroom[4].

**Virtual Courts in India:** The concept of virtual courts is adjudicating cases on virtual online platform. The object of the process is to obviate litigants and lawyers in the courtroom which helped to follow the covid-19 guidelines such as physical distancing given by the government.

In virtual courts, proceedings are done electronically such as e-documents-filing, payment of court fee electronically, arguments are conducted with the help of videoconferencing and the judge presides in proceedings physically in court room or use specified digital platforms within the judicial structure.

The compulsion raised with lockdown directions forced the judiciary to take major steps by effectively using virtual courts across the country to carry out urgent matters. Virtual courts made possible access to justice at any point of time.

Before the covid-19 pandemic virtual courts were limited to specific cases and only few virtual courts started working in the country. But during the pandemic the government in order to provide access to justice to its citizens came up with major reforms by initiating more virtual courts across the country.

---

[4] *Department-Related Parliamentary Standing Committee on Personnel, Public Grievances, Law And Justice Parliament of India, Rajya Sabha Report No.103,2020,http://rajya sabha.nic.in.*

## VII. CHALLENGES OF ICT:

The judiciary system is facing major challenges in implementation of ICT in courtrooms.

**Adopting new technology:** the lawyers and litigants face difficulty to adopt new technology with the digitization of the courtrooms. They were more comfortable with the traditional methods of court proceedings. The technology requires digitization of the data which requires knowledge of the ICT where some of the lawyers feel uncomfortable to adopt new technology.

**Disinterest in E-filing** : In the traditional method the case is filed physically, after digitization of courtrooms most of the stakeholders feel inconvenience with the e-filing due to the technical problems raised while filing a case and which in turn leads to delay in submission.

**Lack of data protection laws**: At present the data protection laws in India are governed by combining statutes and direction. There is no particular data protection law in the country. Government of India proposed a draft bill on data protection which will be a first law to protect personal data shared and received digitally in written and oral format.

**Lack of infrastructure Facilities**: Though the courtrooms are digitized for smooth functioning of judiciary still there is a lack of infrastructure facilities and legal experts with technical knowledge to deal with ICT. As it requires improved internet access and to have various other apps as prescribed by the authorities is more costly.To ensure better implementation of ICT there is a need to provide appropriate training on ICT. Due to lack of knowledge on ICT the stakeholders are facing difficulties to adopt new technology. Fewer online infrastructure facilities and need for data protection laws are the obstacles in better functioning of ICT.

## VIII. CONCLUDING REMARKS

Though it is difficult for some of the stakeholders to adopt new technology but change is the law of the universe, when change occurs unexpectedly in the form of a pandemic it is necessary to find possible opportunities that need to be improved and changed to face the challenges. During the pandemic ICT acted as a catalyst to bring change in every sector affected including the judiciary. Better internet and Wi-Fi connectivity helped in access to justice from anywhere across the nation. Compared to traditional methods e-filing will help to maintain uniformity in the judicial structure across the country. In a physical case filing the litigants face difficulty as the jurisdictions are different from one to another. Forthcoming to the data protection laws, the Indian government is trying its best to bring data protection laws in the country as soon as possible. In a democratic country like India a lot of systematic procedure is involved to bring new legislation. The process of digitization of court rooms are in initial stage and require time to fix proper infrastructure facilities for effective functioning of judiciary. After digitizing efficiency of the Indian judiciary system improved to great extent than any other nation in the world. The phase I, and the phase II (mission Mode e-court project) made significant impact paving a way to the phase III where the new online infrastructure facilities like 5G, internet of things, artificial intelligence, recognition of voice, augmented reality, etc., will be made available to make the judiciary system more efficient and accountable. Pandemic conditions demanded digital transformation which helped to provide justice to public even in crisis situation. The litigants approached courts through virtual mode in urgent matters; this shows the efforts of the government to improve efficiency in the justice delivery system with the help of ICT tools. Decrease in pending cases gained confidence of foreign investors to invest in India. This constructive change brought improvement in India's rank in Ease of doing business index. Thus, implementation of ICT in the judicial system can be viewed asa stepping tool to digitization.

# PEGASUS SPYWARE: EVALUATING THE NEED FOR SURVEILLANCE REFORM AND INTRODUCTION OF DATA PROTECTION BILL

*Sanskriti Shrivastava**
*Muskan Kejriwal***

**ABSTRACT**

*Pegasus attack, an Israel originated spyware, is a "zero click" attack with grants the attacker an ability to infiltrate mobile devices through cyber-attacks, without the knowledge and consent of the target. It then takes control of the target's phone, collect and view its data, access the phone's camera, microphone and target's location.*

*However, the use of cyber weapon and military grade technology such as Pegasus is beyond the powers of electronic surveillance (i.e. interception, monitoring, and decryption) provided under Section 69 of the Information Technology Act, 2000 and falls within the purview of hacking, which is a criminal offence, and have no exception as such. Thus, this paper asserts that Pegasus infractions represent a case of illegal and unconstitutional surveillance. Therefore, in attempt to fill the loopholes in the present legal framework of technological law to deal with the Pegasus attack, this paper shall attempt to provide a solution by critically analysing the present IT Act vis-a-vis need for a surveillance reform and whether or not Pegasus attacks can be included in the definition of "hacking". In view of the same, the*

* *V Year, Student, School of Law, UPES. The author can be contacted at sanskritishrivastava09@gmail.com.*
** *V Year, Student, School of Law, UPES. The author can be contacted atmuskankejriwal31@gmail.com.*

*author shall put forward the controversies and scope of Personal Data Protection Bill and how far it can go to ensure accountability and transparency in a future.*

***Keywords:*** *Pegasus, spyware and its undemocratic use, malware, cyber security, unconstitutional surveillance, hacking, privacy, Information Technology Act, 2000.*

*"If viruses (or spyware like Pegasus) are toppers for cybercrimes, Data is its gold mine."*

*- N.S. Nappinai, Technology Laws Decoded, Lexis Nexis*

## I. INTRODUCTION

On the evening of June 18, 2021, a renowned news agency based in India reported that almost 40 journalists and politicians were targeted in a cyber attack through a non-identified agency by the medium of an Israeli spyware-Pegasus[1].This excerpt made headlines in the subsequent days since the number of targets increased from 40 to more than 300 Indians, not limited to only journalists and politicians.

In response, the Minister of Information Technology and Communications, Mr. Ashwini Vaishnav released a parliamentary statement on July 18, 2021 clarifying non-involvement of government or any of its agency behind such attack[2]. It also proposed to investigate the alleged cyber attack to conform whether the targeted people have actually been attacked or just been a subject of an attempt attack. Following this, India witnessed a situation of havoc and apprehension among general public since their location, text messages, calls, search history and other sensitive information was allegedly put to the mercy of this spyware attack.

---

[1] Anuj Srivas and Kabir Agarwal, *Snoop List Has 40 Indian Journalists, Forensic Tests Confirm Presence of Pegasus Spyware on Some*, THE WIRE (July 18, 2021),https://thewire.in/media/pegasus-project-spyware-indian-journalists.

[2] Ministry of Electronics and IT, *Alleged use of spyware Pegasus to compromise phone data of some persons*, (July 18, 2021)https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1736803.

Additionally, the use of Pegasus lacked legal sanction and therefore it violated the democratic structure of India and threatened data privacy concerns among other specific legislations. This article argues that the present legal framework including IT Act and the Telegraph Act, 1885 are incompetent to bring Pegasus within the four walls of legal scrutiny. Further the article also discusses the relevance of the Protection of Data Privacy Bill, 2019 *(hereinafter referred as "PDP")*in the present context.

## II. PEGASUS IS A CYBER ASSAULT OVER ONE'S PRIVACY

The critical features of Pegasus give it an ability to snoop into the privacy of its target without its due consent has created an apprehension of privacy risk. In India, multiple renowned politicians, journalists and bureaucrats were targeted which created apprehension of digital assault in the minds of general public as well.

While the Indian society is familiar with the authorized snooping, it has witnessed an unethical use of suave technology for the first time. Interestingly, the authorized surveillance which was meant to keep a check on defense and national affairs have widened itself to include anti-governmental affairs as well.

Further, in response to the ongoing controversies the Information Technology Ministry have segregated the legal concerns arising out of this spyware and has maintained a defined stand throughout[3]. It relies upon the existence of law, to protect privacy and to authorize lawful surveillance. Further, it went to disintegrate the alleged compromise with the privacy as an attempt to compromise on a real one.[4]

However, the point of concern remains intact. One, till date there is no provision in the black letter which directly talks about infringement of digital privacy and its relevant remedy. Two, there is no law in place which gives a clear transparent demarcation between authorized and unauthorized surveillance and its allied ambit.

[3] *Id.*
[4] *Id.*

In fact, the existing gaps between the present incompetent legal framework including the Telegraph Act, 1885 and Information Technology Law, 2000 aids such unauthorized snooping and invasion into an individual's privacy. The scope of the protection of one's privacy has been constantly argued before different judicial bodies in India. In fact, it has been carefully curated where phone tapping and unethical and unreasonable surveillance were held contrary to the fundamental rights.[5] In 1996, a Delhi Based Non-Profit Organization- People's Union for Civil Liberties challenged constitutionality of Section 5(2), Telegraph Act which allows authorized interception.[6]Whilst the Hon'ble Apex Court did not stuck down the concerned provision it stressed upon *'unreasonable intervention into one's privacy'* where the data surveillance was not duly authorized. It further went on to observe that interception can only be called as an "authorized" one when either it is in the interest of public safety or it involves a condition of public emergency.[7]

Recently, in a landmark holding, the Hon'ble Supreme Court of India widened the interpretation of Article 21 so as to include right to privacy within its ambit and highlighted that *"an individual possesses a control over his personal data…and his existence on the internet"*[8]. Therefore, attacks like Pegasus infringes the cardinal fundamental right guaranteed by Article 21, Constitution of India.

Nonetheless, none of the above two landmark decisions concerning data privacy fits perfectly into the square of Pegasus. The issues of unauthorized surveillance and transgression of privacy also hinders with the very ideas of liberty and dignity, pursuant to the preamble of the Constitution of India. This spyware is in the nature of "zero detectable" format of surveillance and is a dire threat over the basic notions of India being a democratic nation. In fact, the absence of relevant, credible and accountable legal framework upon the concerns of digital invasion into privacy, compromises with the

[5] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[6] *Id.*
[7] *Id.*
[8] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

sovereignty and national interest and exposes the target to cyber vulnerability.

## III. RELEVANT PROVISIONS UNDER THE IT ACT, 2000

The IT Act is a primary Information Technology legislation in India. It is an act of parliament which is aimed at giving legal recognition to Electronic Documents and Digital Signatures. However, The IT Act, 2000 was insufficient to fulfill its objectives because of the gaps in the provisions. It attracted gaze from both the industries (who called it a "draconian law") and from the general public (who called it "lenient"). This led to the need for an amendment in the Act, which was aimed to address the potential shortcomings of the IT Act, 2000. Thereafter, major advisory bodies were formed to recommend changes in the Act of 2000, after which, we had the Information Technology (Amendment) Act, 2008, which got presidential assent on 05 February 2009 and accordingly, commenced on 27th October 2009.

IT Act is concerned about both data and information. Data has no meaning in itself; however, information is a data with meaning. This means, data are mere raw facts and information adds value to the data. Section 2(1)(v) of the IT Act defines "information" so as to cover data, messages, text, image, sound, voice etc. basically, every piece of information which is computer generated is covered under the ambit of IT Act. Section 2(1)(o) of the Act defines "data" so as to include a representation of any facts or information, that is prepared and is intended to be processed in a computer system

Nonetheless, the Pegasus cyber-attacks once again highlight the incompetency of the IT Act, along with the 2008 amendments. One of the interesting features of this Act is that it empowers the Central Government to conduct authorized surveillance, i.e., it can *"intercept, monitor and decrypt"* any information belonging to any individual. Since the government has not admitted the usage of Pegasus, the invocation and scope of this provision is controversial.

Further, Information Technology Rules, 2009[9] *(hereinafter referred as "IT Rules, 2009")* defines interception to include all the manners which involved interception devices whereas monitoring involves monitoring devices. Nonetheless, it is apprehended that the threshold of stipulated monitoring devices and interception devices may not be satisfied by the equipment used in cyber-attacks through Pegasus.

Further, even if, we consider the surveillance issue at hand within the ambit of IT Rules, 2009 the act must confirm with the pre-conditions mentioned therein to be termed as "authorized". These conditions are- (1) existence of a prior permission by way of a reasoned order through Central or State Government;[10] (2) this order passed by the Central or the State Government remains in force only for a period of 60-180 days[11]and (3) Such orders are subject to review by a review committee which is set up by the Central Government for this purpose.[12]

Furthermore, this part critically analyses the power of central government to "intercept, monitor or decrypt data" pursuant to Section 69 of the IT Act (3.1.) and thereafter contends that penalties mentioned under Section 43 read with section 66B of the IT Act is insufficient to squarely cover the havoc created by Pegasus (3.2.).

**Section 69 of the IT Act, 2000-**

Section 69 of the IT Act empowers the government to put information of any individual(s) on authorized surveillance. This provision directs towards the lenient area of the Act which is aimed to protect lawful and reasonable surveillance which is necessary in national interest. Its primary aim is to authorize the acts which protects the sovereignty, integrity and security of India or which facilitates observance of public order and continuation of

[9] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules,2009(India).
[10] *Id, Rule 4.*
[11] *Id, Rule 11.*
[12] *Id, Rule 12.*

friendly relations with other countries. However, the attack of Pegasus on general public has inked the controversy and interpretation of this provision.

Pegasus spyware was targeted at the anti-government elements and not against the anti-national elements. This irked controversy about the scope of Section 69 of the Act, i.e. whether it covers authorized surveillance meant to curb anti-national elements or has it widened itself to cover anti-government elements as well. However, before criticizing the ambit of Section 69 of the Act, it is necessary for the government to admit its invocation in the given context. Only when the alleged provision is said to be invoked, can its ambit be argued. Nonetheless, the IT Ministry has not yet clarified whether or not it has invoked this provision and has alternatively maintained a position of incomprehension about the usage of Pegasus.

**SECTION 43 READ WITH SECTION 66 AND 66B of IT Act, 2000-**

Section 43 of the IT Act lists ten instances where if any individual access, downloads or conducts any activity incidental thereto with a computer (including computer network) without due consent of its owner or the person in charge, he shall be liable to compensate the person so affected whereas Section 66B of the IT Act provides for punishment for related matters.

Therefore, a conjoint reading of the mentioned provisions suggests that if a person dishonestly commits an act mentioned under Section 43 of the IT Act, he shall be liable for an imprisonment which may extend upto 3 years or with fine up worth Rs. 5 Lakh or both under Section 66B of the Act.[13] The ten stipulated instances under Section 43 of the IT Act includes the act of accessing a computer/ computer network without consent,[14] disruption or damaging of a computer device/network,[15] denial of access to a duly authorized person,[16] destruction or alteration of any information present

[13] Information Technology Act, 2000, No. 21, §66B; Acts of Parliament, 2000 (India).
[14] *Id, §43(a).*
[15] *Id, §43(d).*
[16] *Id, §43(f).*

therein[17], downloading/copying of data without consent[18] and concealing or destruction of computer source code.[19]

It is undebated that the impact of Pegasus results into non-consensual snooping into an individual's mobile device. It enables the attacker to dishonestly or fraudulently access the mobile device, download, copy, destroy or alter the data of its target phone. Therefore, it can be said to be indirectly covered under Section 43 of the Act.[20]

However, neither section 43 and 66 nor section 66B mention the term "mobile device" and only provides about "computer networks" and "computer system". The Act defines a "computer" as any electronic data processing device capable of performing logical, arithmetic and memory functions.[21] "Computer network" is further referred as an inter-connection between two or more computers[22] whereas "computer system" has been given a wide meaning so as to include a device containing computer programmes.[23]

Therefore, on the basis of technicalities involved and the inherent differences in the functioning of a mobile device and a computer system it is blurry whether or not the former can be included within the ambit of the latter under the IT Act. Alternatively, it can be said that the impact of Pegasus is well covered within the ambit of Section 43 read with Section 66 of the Act. However, the inclusion of the medium by which Pegasus attacks its target i.e., a mobile device - is still doubtful.

## IV. THE TELEGRAPH ACT, 1885

Government has been empowered under Section 5(2) of the Telegraph Act to direct interception of a message when it considers it to be in the interest of

---

[17] *Id, §43(i).*
[18] *Id, §43(b).*
[19] *Id, §43(j).*
[20] Shreya Singhal v. UOI (2015) 5 SCC 1.
[21] *Supra* note 13 at §2(i).
[22] *Id*, §2(1)(j).
[23] *Id, §2(1)(l).*

the "sovereignty and integrity of India"; "the security of the State"; "friendly relations with foreign states"; "public order"; for "preventing incitement to the commission of an offence. "An interpretation of the above provision *prima facie* suggests that the executive has been granted wide arbitrary powers under the Telegraph Act, 1885. This is based on the fact that the provision does not provide for any safeguards against the surveillance which serves the purpose of achieving any political ends or has mala-fide intentions. It is pertinent to mention here that the underlying reason behind absence of safeguards is done in order to achieve mala fide intentions and fulfill political agendas thereby creating an intrusion of right to privacy. Further, when the privacy of an individual is infringed through surveillance by the government, the individual who is made the target is not even aware of such evasion and therefore it cannot be expected from him to seek any remedy.

Therefore, in such cases, the system of checks and balances upon the mala fide intentions of the government is not maintained by the Constitutional Courts which acts as the custodian of citizen's fundamental right. Rather the government authorities are the sole body to decide whether or not any reasonable grounds exist for the surveillance leaving no scope for judicial scrutiny.

This invasion may result in dangerous outcomes when government keeps shriveling for a number of years without any judicial intervention by the Courts and also doesn't provide any reasonable opportunity to the individuals who are subject to such invalid surveillance to protect them. The loophole which exists in the present legislation is that it does not provide for any scope to differentiate constitutionally "permissible surveillance" from "impermissible surveillance".

Although, the loophole has been found but what requires to be considered is the solution which can bridge a gap in the current legislation which has given immense arbitrary powers to the government without being subjected to any judicial review.

It is further stressed that the judiciary has always acted as the protector of citizen's right granted to them under the Constitution and has thus served the objective of protecting the individuals against impermissible surveillance and the solution in the present scenario which can be considered effective is to set up a Tribunal or a Special court which will be an independent body to grant permission and to examine whether or not the grounds exist for mandatory surveillance. By this, the surveillance aimed at achieving any political goals and is with mala fide intention should not be allowed.

Moreover, as there are no provisions which stipulate the period for which the government can carry on the surveillance secretly making the provisions of Telegraph Act, 1885 arbitrary. The Tribunal body would decide on such time period and would also examine the profile of the individual, his criminal antecedents, any conflict history with government etc, in order to decide whether shrivelling such person is in general public interest or not.

## V. PERSONAL DATA (PROTECTION) BILL, 2020

In today's technological dynamic environment people all around the world are connected by an intangible force of the Internet and the power to access the world lies at the hands of different entities which ranges from mighty governments to successful corporate entities to individual citizens. Although such powers has been vested in these entities but there is always a possibility wherein the power and knowledge are misused which would ultimately weaponries the very identities of vast swathes of people in the world.

The PDP Bill is in the process of being tabled to enhance the privacy laws in India and to give legislative backing to the judicially recognized right to privacy (which includes right to the protection of data), as held in *Puttuswamy v. Union of India*.[24]

Thus, the PDP Bill, 2019 was introduced with an objective and intention of taking another step to recognize the fundamental right to privacy as

[24] S*upra*note8.

recognized in *Puttuswamy*. The Bill proposes certain measures which the data fiduciary must comply while processing the personal data.

Section 4 of the bill states that "no personal data shall be processed by any person, except for any specific, explicit, and lawful purpose."[25]

Section 5 states that "the processing by the data principal must be done in a fairly and reasonably keeping in mind the privacy of the data principal (i.e., the person providing the data), and for the purpose that was consented to by the data principal."[26]

Section 6 states that "personal data shall only be collected to the extent that is necessary for processing such personal data."[27]

Section 7 importantly talks about all the information that the data principal must be intimated of by the data fiduciary regarding the collection of the information while it is collecting personal data. The purposes for processing of data includes nature of such data and details like identity and contact details of the fiduciary, etc.[28]An important clause, clause (d) of Sub-section (1) states that "the data fiduciary must give the principal notice of the right of principal to withdraw consent and the procedure for withdrawal of consent, if the data is to be processed on the basis of such consent".

Section 35 of the Personal Data Protection Bill, 2019[29] also becomes relevant in this context as it states that "where the Central Government is satisfied that it is necessary, it may, for certain reasons which must be recorded, direct that some or all of the provisions of the PDP Act, (when/if it does become one) will not apply to the agency in question, which reeks of arbitrariness."

---

[25] Personal Data Protection Bill, 2019,§4.
[26] *Id,* §*5.*
[27] *Id,* §*6.*
[28] *Id,* §*7.*
[29] *Id,* §*35.*

However, there exists a gap in both these provisions and *the PUCL's case* can be questioned on the ground that none of these provisions provides for a reliable *"procedural safeguard against abuse or interference with rights,"* as laid down by Kaul, J. in the *Puttuswamy* judgment. The above-mentioned provisions provide power of exclusion of agencies from restrictions of the PDP Bill, tracing of data by fiduciary, etc. to the government but does not provide for any judicial review of the same and thus does not leave any or enough procedural safeguards to prevent against violation of fundamental right to privacy. Although *PUCL* stipulates approval from the Home Minister, but this approval ultimately is an executive function and does not honour the division of power, thus opening the doors for possible misuse by the Executive. Warrantless surveillance is also permitted under the Act and Rules, therefore removing any chance of judicial intervention.

Thus, with regards to *Pegasus spyware scandal* there has been an intense speculation about the possibility of the Indian government having sanctioned the usage of the spyware on the 121 people in India who have been affected by it.[30]As discussed above, Pegasus was spyware software developed by Israel-based NSO Group, which affected multiple devices all over the world, especially those of Human Rights activists, lawyers, etc., and stole data related to chats, calls, etc. on their WhatsApp accounts. In light of NSO's declaration that it sold the software only to Governments around the world, and what has been perceived as a less-than- satisfactory response by the Home Ministry[31] to questions regarding its complicity, the question must be asked – if the government did in fact authorize the deployment of Pegasus, is it within the law in having done so?

Further, Rule 12 of the IT Rules 2009[32] states that "the authorized agency shall designate a nodal officer who will send a requisition conveying the

[30] Rajeev Deshpande, *Pegasus attacked 121 in India, breached 20: WhatsApp to Government*, THE TIMES OF INDIA, https://timesofindia.indiatimes.com/india/pegasus-attacked-121-in-india-breached-20-whatsapp-to-government/articleshow/72192198.cms.

[31] Meryl Sebastian, *Did Indian Government Buy Pegasus Spyware? Home Ministry's Answer Is Worrying*, HUFF POST,https://www.huffingtonpost.in/entry/did-indian-govt-buy-pegasus-spyware-home-ministry-answer-is-worrying_in_5dd3bbb1e4b082dae813a058.[2] Rule 12, *Supra* note at 9.

direction for interception, monitoring or decryption to the *designated officers of theconcerned intermediaries or the person-in-charge of the computer resource."* In the case of WhatsApp and its data, WhatsApp constitutes as the intermediary, and since the only encryption key available is present with the users of WhatsApp and the information, even at rest, is available only with the users of WhatsApp (not being stored in their servers except in exceptional circumstances), the users of WhatsApp would constitute the "persons in-charge" of the computer resource.

In fact, In the WhatsApp-Pegasus leak, WhatsApp, which acted as an intermediary, has made clear that it did not authorize or allow the attack or any leak of personal data. In that case, if the government actually had somehow authorized the attack, it is, in all probability, on the wrong side of the law.

### A. Right to be Forgotten

One of the right recognized under the right to privacy is the Right to be Forgotten and is recognized by various multiple international agreements and laws like the General Data Protection Regulations, 2016 *(hereinafter referred as "GDPR")* which gives the data subject the right to request the controller (herein the "data fiduciary" as per the PDP Bill ) to erase personal data concerning him or her without undue delay where certain grounds like lack of necessity, withdrawal of consent, etc. are applicable. The PDP Bill also acknowledges the Right to be Forgotten, with Section 20 of the Bill stating that "the data principal shall have the right to restrict or prevent" the "continued disclosure" of personal data by the fiduciary, and lists certain reasons which will make it applicable. The PDP Bill differs from the GDPR on the ground that GDPR has a bigger list of reasons for which the right to be forgotten can be invoked, like, under clause (c), if the data subject (data principal) objects to the processing pursuant to Article 21 (right to object), *inter alia*.

Kaul, J. in *Puttuswamy* explicitly identified the right to be forgotten, in physical and virtual spaces, under the ambit of right to privacy as a fundamental right. Kaul stated, *"The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet"*. This ties into his reasoning that the public does not have a claim to access all truthful information.

However, one must consider that such right is not unrestricted and is subject to public interest, compliance with legal obligations and duties like public health, taxes, scientific research etc. However, PDP Bill and the judgments is still vague and unclear about the ambit of such right and its extent and whether or not it would extend only to removing search engine result or would it extend to removing the origin of such search engine hit?[33]

This issue was observed in *Sri Vasunathan v. Registrar*[34], where the Court, though while recognizing this right also extended the remedy only to the copies of the order yielded in the internet search and not the source documents them. Going farther than this would also yield logistical difficulties in the form of tracking down domains which name the person and instructing them to remove the document or the mention of the name of the person in the document. There is also no solid legislative backing to the principle, with neither the IT Act nor the Rules pointing to a direct reference (the PDP Bill does have a reference to it, but has not been passed), as was pointed out in *Dharamraj Dave v. State of Gujarat*[35], where the court expressed a dearth of legislative backing to the argument that a publication of a non-reported case by a website must not be allowed.

Whether WhatsApp complies with this Right to be forgotten is not completely clear, though it definitely is expected to, in order to be compliant

[33] Sohini Chatterjee, *In India's Right to Privacy, a Glimpse of a Right to be Forgotten*, THE WIRE, https://thewire.in/law/right-to-privacy-a-glimpse-of-a-right-to-be-forgotten.
[34] Sri Vasunathan v. The Registrar General 2017 SCC OnLine Kar 424.
[35] Dharamraj Dave v. State of Gujarat 2015 SCC OnLineGuj 2019.

with the GDPR. WhatsApp's Privacy Policy, under the head "Deleting your WhatsApp Account" states that *"When you delete your WhatsApp account, your undelivered messages are deleted from our servers as well as any of your other information we no longer need to operate and provide our Services. Be mindful that if you only delete our Services from your device without using our in-app delete my account feature, your information may be stored with us for a longer period."* The wording that information no longer needed to operate services will be deleted, may imply that, upon WhatsApp's discretion, some information that may be necessary for their functioning may be retained, even though the user has withdrawn consent to WhatsApp to use his/her data. This may be a violation of the Right to be forgotten.

### B. Critique

Although there was a hope that the data protection bill will improve the status of the individuals concerning their data privacy in India and that if the Personal Data Protection Bill, 2019 (herein PDP Bill), if passed will provide or facilitate in providing a remedy or an avenue to the affected parties of Pegasus malware a right to seek legal redressal. However, the PDP Bill and the principles and provisions which have been stipulated therein provides for many exceptions and exemptions to executive authorities and as such represents a missed opportunity for surveillance reform.

Moreover, broad exemptions which has been provided to law enforcement and intelligence agencies in India as enshrined in Clause 35 of the PDP bill are very vague and arbitrary as it exempts the state authorities from the application of the PDP Bill if it is proved that the surveillance is "expedient" or "necessary" to do in the interest of national security, public order, friendly relations with foreign states, or to prevent the commission of certain offences. Further, such exemption order can be made by the government without any judicial or parliamentary approval.

Similarly, Clause 36 also provides for broad exemptions to state and private players who process personal data to prevent, detect or to investigate or prosecute any person under "an offence which in contravention of any law" for the time being in force.

Additionally, PDP Bill also does not provide for any "necessary" or "proportionality" test propounded in *Puttaswamy c*ase which the law enforcement agencies must meet which invoking the exceptions are stipulated in the Bill.

Therefore, from the above-mentioned factors, relying on the PDP bill that it may provide sufficient remedy and as such exercise of ensuring accountability and transparency in a future Pegasus case may prove to be pointless and in vain.

## VI. CON CLUSION

Pegasus spyware has left the entire cyber law community with goose bumps. It has practically threatened and infringed the basic notions of privacy which are well settled in the Indian legal system. In 21st century where the technology is hyper competitive, the law shall leave no stone unturned which could actively or passively apprehend the privacy of individuals.

Data leaks in this scandal have clearly shot an arrow into one's private space, infringing Article 21of the Constitution of India along with the notions of liberty and democracy established therein. The current legislation is incompetent to cover the notorious impact of this spyware. IT Act, the primary cyber law legislation in India, puts forth Section 43, 66, and 66B which could passively cover the violations caused by Pegasus. However, the technicalities and prerequisites of a computer system or computer network might not be fully met herein where the attack takes place through a mobile device.

Further, it is futile to argue the ambit of Section 69 of the IT Act since its invocation is still inexplicit from the purview of the government. Even if one

argues that Pegasus snooping was an authorized one, it lacks any reasoned order to that effect making it an arbitrary move.

Furthermore, another relevant legislation, the Telegraph Act 1885, provides a very narrow ambit to remedy violations done by Pegasus. Additionally, it does not provide any guidance to differentiate between a permissible and an impermissible surveillance. This leaves a constant rift between the executive and judiciary pointing towards a delicate drift over the concept of separation of powers.

Lastly, the seemingly promising PDP Bill has daunt the entire cyber law committee because it has left the government with arbitrary powers. It is apposite to mention here that the PDP Bill has not touched the mark of procedural safeguards as laid down in the celebrated *Puttuswamy Case*.

Therefore, this article argues that the act of snooping into the mobile phones of over 300 Indians were an unreasonable intervention into the privacy of the targets and lacked the force of legal sanction. It further contends that the insufficiency of the present legal framework facilitates more aggravated forms of such attacks in the future and leaves the target without any remedy. This situation has indeed unturned the idea of '*ubi jus ibiremedium*' because the existence of right to privacy is undeniable, yet law encompasses no remedy to the aggrieved party.

POLICY BRIEF

# ONLINE EDUCATION: ANALYSING THE EXCLUSION OF INCLUSIVITY FROM THE PRISM OF CHILDREN WITH DISABILITIES

Dr. Marisport A.*
Gauransh Gaur**

**ABSTRACT**

*The pandemic of the coronavirus has begun a new chapter in virtual learning. However, the advantages of virtual learning do not obscure the exclusive aspect of this learning, which is exacerbated by our society's existing digital divide.[1] In current society, inaccessibility to digital education is not unusual. Individuals' ability to learn digitally is influenced by their economical, physical, and social circumstances.[2] These factors play a significant influence in deciding how digital learning is distributed in society. There are many people who are unable to obtain the appropriate education in these difficult times.[3] Despite being such low rates, unfortunately their concerns are not brought in the mainstream, and their problems are kept getting ignored. Through this article, the authors would examine the legal obligations of the state in ensuring the inclusive education for the disabled students by analysing the recent findings of various research studies highlighting the difficulties faced by the disabled students in accessing online education and study the e-content guidelines issued by the government for making online content available for every disabled student. The article will explain the issues left unaddressed in the*

*Assistant Professor of Law at Gujarat National Law University (GNLU). The author can be contacted atmarisport@gnlu.ac.in.
**B.Com. LL.B. (Hons.), Gujarat National Law University (GNLU).The author can be contacted atgauransh.gaur30@gmail.com.

*way of inclusive education and conclude with the recommendations for achieving the goal of inclusive virtual education.*

***KEYWORDS:*** *COVID-19 pandemic, disabled students, legal obligation of the state, online learning, unaddressed issues of inclusive virtual education.*

## I. THE LEGAL NORMS ON INCLUSIVITY

India has been the signatory to the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD), 2006. In order to realize the objectives and commitments of the same convention, domestic legislation (Rights of Persons with Disabilities Act, 2016) was enacted. Same UNCRPD convention obliges the state to take full measures in ensuring the accessibility to resources by persons with disabilities. Article 9 of the convention requires the state to take measures for eliminating the obstacles and barriers that comes in the way of persons with disabilities.[4] Similarly, state is bound to provide assistance in form of "guides, readers and professional sign language interpreters", and has the obligation to promote the accessibility to "new information and communications technologies and systems, including the Internet".[5]

Similarly, article 24 of the Convention directs that "Persons with disabilities are not excluded from the general education system on the basis of disability, and that children with disabilities are not excluded from free and compulsory primary education, or from secondary education, on the basis of disability".[6] They must be given access to "inclusive, quality and free primary and education", and reasonable accommodation should be provided to them

---

[1] *As digital divide widens, India risks losing a generation to pandemic disruption*, THE PRINT, https://theprint.in/india/education/as-digital-divide-widens-india-risks-losing-a-generation-to-pandemic-disruption/568394/ (last visited 1 July 2021).

[2] Unni, J. C., *Social Effects of COVID-19 Pandemic on Children in India. Indian Journal of Practical Pediatrics*, 2020,22(2), 213.

[3] *Id.*

[4] Art. 9 & Art.3, THE UNITED NATIONS CONVENTION ON THE RIGHTS OF PERSONS WITH DISABILITIES (UNCRPD), May 2008.

[5] *Id.*

[6] Art. 24, THE UNITED NATIONS CONVENTION ON THE RIGHTS OF PERSONS WITH DISABILITIES (UNCRPD), 3May 2008, a/res/61/106.

whenever required.[7] Further, appropriate measures are required by the state to empower teachers qualified in teaching children with disabilities to get themselves to be upgraded with sufficient training.

Apart from these commitments in UNCRPD, the State has certain obligations in the domestic legislations also. The Indian Constitution guarantees the right to life to every citizen under Article 21. This includes access to education for self-development of the children with disabilities. Further, the RPwD Act defines the system of inclusive education as "enable persons with disabilities to learn life and social development skills to facilitate their full and equal participation in education and as members of the community."[8] Section 17 of the Act directs the government to undertake appropriate measures for promoting and facilitating the inclusive education.[9] Almost every obligation mentioned under the UNCRPD is given in this act. Further, Web Content Accessibility Guidelines (WCAG) provides myriad of recommendations for making web content accessible for students with disabilities.[10] All websites run by Government of India has necessary adjustments to enable persons with disabilities to read, perceive, see, and understand the web content. These guidelines are called GIGAW (Guidelines for Indian Government Websites).[11]

## II. THE GROUND REALITY

The children with disabilities constitute the "largest out-of-school segment with the highest dropout rates".[12] When the pandemic has almost shut the door for physical classroom, online platforms like Zoom, Webex, Google Meet have become the new classroom for students. However, not all these platforms are accessible for students with disabilities. Sometimes, the link

---

[7] *Id.*
[8] Rights of Persons with Disabilities Act, 2016, § 2(m), No. 49, Acts of Parliament, 2016 (India).
[9] Rights of Persons with Disabilities Act, 2016, § 17, No. 49, Acts of Parliament, 2016 (India).
[10] WEB GUIDELINES, https://web.guidelines.gov.in/1-8-accessibility (last visited 12 July 2021).
[11] *Id.*
[12]THE WIRE,https://thewire.in/rights/virtual-learning-children-with-special-needs (last visited 1 July 2021).

for an online class is inaccessible for the screen reader to configure.[13] Even the presentations and materials presented during the online classes are not accessible for the students with disabilities very often. [14]Unfortunately some intellectually disabled students have to face drop outs from educational institutions due to lack of understanding in the online classes.[15] Similarly no language interpreters for deaf students is provided in every class, and students wearing prosthetic limbs are unable to type effectively as other students.[16] Challenges like these have prevented the holistic learning of students with disabilities. A study conducted by Vidhi, titled *Vidhi, COVID-19 and Exclusion of Children with Disabilities from Education*[17] found that "62% of students with disabilities were 'never', or only 'sometimes' able to understand the lessons and finish their assignments, due to inaccessibility". In a survey conducted by Swabhiman – a community-based organization, and the disability legislation unit of eastern India of the National Centre for Promotion of Employment for Disabled People.[18] It has been brought out that majority of these students are facing problems during online learning. Majority of the students (56.5%) admitted that they were struggling with the online classes, however they kept on attending.[19] While almost 77% of them feared that they would lag behind in learning, and would be unable to cope up due to their inaccessibility to digital education.[20]

---

[13] SMASHING MAGAZINE, https://www.smashingmagazine.com/2020/06/accessible-video-conferencing-tools/ (last visited 11 July 2021).

[14]*As 'unlockdown' starts, persons with disabilities face fresh challenges*, INDIAN EXPRESS, https://indianexpress.com/article/lifestyle/life-style/persons-with-disabilities-unlock-1-challenges-social-distancing-inaccessible-apps-work-from-home-6477913/ (last visited 12 July 2021).

[15] INDIAN EXPRESS, https://indianexpress.com/article/education/students-with-intellectual-disability-hit-hard-by-covid-19-lockdown-7077265/ (last visited 22 July 2021).

[16] EDEXLIVE, https://www.edexlive.com/news/2020/jun/21/students-with-disabilities-having-harrowing-time-trying-to-access-online-classes-demand-better-acce-12773.html (last visited 22 July 2021).

[17] *COVID-19 and Exclusion of Children with Disabilities in Education,*VIDHI CENTRE FOR LEGAL POLICY, (Dec 8 2020). https://vidhilegalpolicy.in/wp-content/uploads/2020/12/Vidhi-Report_Inclusive-Education-Full.docx.

[18]THE HINDU, https://www.thehindu.com/news/national/karnataka/coronavirus-lockdown-students-with-disabilities-struggle-with-online-classes/article32126029.ece (last visited 3 July 2021).

[19] *Id.*

[20] *Id.*

The parents of around 90 percent of these students complained about the lack of attention given by the teachers to their children with special needs.[21] Further, technological divide is also highlighted through this survey where a majority of the parents (86%) expressed that they were unable to use the technology properly.[22]

A significant percentage (81%) of the teachers has expressed their concerns while stating that they are unable to have an access to online educational materials for the children with disabilities.[23] On the similar line, many teachers (64%) were not given having the access to smart phones and computers or laptops for providing the education from home.[24]

Many students (77%) have complained that lack of educational materials in accessible format is coming in their way of online learning.[25] Poor internet connection was also one of the impediments which stalled their learning during the tough times as almost two –third of the students expressed the need for proper internet connection or Wifi for an uninterrupted learning.

Moreover, the online learning has presented the challenge for these students as they are unable to get the services of scribes, sign language interpreters, and readers. During the online webinars, almost half of the students highlighted about the absence of sign language interpreters. Similarly, students are facing the problems of getting the scribe for their online examinations during the pandemic.[26]

Further, teachers have also faced significant challenges during the pandemic, which has impacted the education of students with disabilities. Many teachers at the inclusive schools were given the additional responsibilities of

---

[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] NEW INDIAN EXPRESS, https://www.newindianexpress.com/states/tamil-nadu/2020/dec/23/visually-impaired-students-struggling-sans-scribes-to-take-remote-exams-2240050.html (last visited 10 July 2021).

relief work during the time of pandemic.[27] Additionally, they also faced economic insecurity due to the delay in payment of remuneration or salaries. Further, just like students, teachers also face difficulties in navigation on online modes of learning, and consequently rely immensely on parental engagement.[28]

## III. RELEASE OF E-CONTENT GUIDELINES

With an aim of making education inclusive for disabled students, the government has recently released the "Guidelines for the Development of e-Content for Children with Disabilities".[29] The digital content for disabled students would be based upon the 4 principles: "perceivable, operable, understandable and robust".[30]The content including videos, text, diagrams, graphs, audios, etc would be in compliance with the accessibility standards followed nationally (GIGW 2.0) and internationally (WCAG 2.1, E-Pub, DAISY) etc.[31]

Technical standards should be followed on the digital platforms (like DIKSHA), and reading platforms where the online content would be uploaded. To meet the special needs of the disabled children or students, reasonable accommodations in pedagogy would have to be done.[32]

In a phase wise manner, textbooks for these students would be made available in Accessible Digital Textbooks (ADTs), where the content would be given in variety of formats (visuals, audio, sign language, video, etc.) with the feature of on and off.[33] Thus, disabled students would be given the flexibility in studying the content in different ways.

---

[27] *COVID-19 and Exclusion of Children with Disabilities in Education, Vidhi Centre for Legal Policy*, (Dec 12 2020), https://vidhilegalpolicy.in/wp-content/uploads/2020/12/Vidhi-Report_Inclusive-Education-Full.docx.

[28] *Id.*

[29] *Guidelines for the Development of e-Content for Children with Disabilities*,https://www.education.gov.in/sites/upload_files/mhrd/files/CWSN_EContent_guidelines.pdf (last visited 10 July 2021).

[30] PIB, https://pib.gov.in/PressReleasePage.aspx?PRID=1725279 (last visited 10 July 2021).

[31] *Supra* note 20.

[32] *Id.*

[33] *Id.*

Further, there are also detailed guidelines available for generating the accessible digital textbooks of various international and national books. In addition to these books, supplementary of e-content would also be made available for 21 disabilities as mentioned under the RPwD act 2016 for their growth and development.[34] This feature would foster the skills of "students having Intellectual and Developmental Disabilities, Multiple Disabilities, Autism Spectrum Disorders, Specific Learning Disabilities, Blindness, low vision, Deafness and Hard of Hearing and others."[35]At last, the Section 10 of the report also provides with a list of recommendations for the content creators, publishers, developers for making the disability-friendly content. An implementation road map is also provided in Section 11 for ensuring strong compliance with these guidelines. The report concludes with the guidelines for producing the content using the sign language and making pedagogical accommodations in one's approach.

## IV. ISSUES LEFT UNADDRESSED

Though the guidelines have sufficiently addressed the problem of inaccessible digital content among the disabled children or students, there is still a need to address the high dropout rates among the disabled children as almost half of the children, as per the survey done by Swabhiman NGO[36] are leaving the educational institutions due to the hurdles in online education. Lack of training among the children with disabilities makes them unable to access the distance learning modes.[37] Children are unable to access the online classes, digital content, and other reference material.

Further, a lot of these things are managed by the parents of these children who generally do not have sufficient technical knowledge in accessing the

[34] Rights of Persons with Disabilities Act, 2016, § 2(zc), No. 49, Acts of Parliament, 2016 (India).
[35] *Id.*
[36] THE HINDU, https://www.thehindu.com/news/national/43-children-with-disabilities-planning-to-drop-out-due-to-difficulties-faced-in-e-education survey/article32121145.ece#:~:text=About%2043%25%20of%20children%20with,survey%20conducted%20with%203%2C627%20respondents.&text=The%20survey%20found%20that%2056.48,are%20planning%20to%20drop%20out (last visited :11 July 2021).
[37] *Supra* note 20.

online classes and other related things.[38] A significant number of disabled students are facing difficulty in understanding the topics during the online classes.[39] It may happen that special care which was earlier given to these students in physical classes might get reduced due to the less number of online classes available. Further, special lectures or remedial classes which were earlier used to be given to these students may also get reduced due to the pandemic, which might be hampering their learning, and consequently most of the students are forced to drop out as they lag behind gradually.

The teachers must ensure that students with disabilities are able to understand all lessons clearly, and adequate attention should be given to them during the classes so that they should not be left behind due to the online classes. Further, remedial classes and special lectures should not be reduced in these tough times for these students.

Strict mechanisms should be installed to check whether these accommodations are being learnt by the teachers at a sufficient pace, and whether these accommodations are being practiced at the ground level. Similarly, the teachers are also unable to access the digital classes and online content which hurdles the flow of learning in a class. Lack of technical knowledge at every front; teacher, students, and parents, as per the reports,[40] are disturbing the pace of learning in the digital education.

Further, the rise of online education has also brought to light the digital divide that exists in the society. This digital divide is more rampant in the rural areas where the villages do not even have the proper internet towers. Another issue that is ancillary to this problem is the lack of sufficient devices for attending the classes. It may happen those mobile phones and other device are only available for a limited period, and then it is used for other purpose. In this way, a disabled child is unable to attend his entire classes.

---

[38] *Id.*
[39] *Id.*
[40] *Id.*

As mentioned earlier, the survey done by Swabhiman NGO has highlighted the disparity in resources among the teachers also, "the teachers also reported that 64 % of students (CwD) did not have smart phones or computers at home. As many as 67% of students (CwD) said they needed tabs or computers or comparable devices for online education.....About 74% of children with disabilities said they needed data/Wi-fi support for educational purposes..".[41]The coronavirus pandemic has switched the physical classroom learning model to the virtual one. However, this model has restricted its access to the people who are having technical resources at their disposal.

There is an urgent need to ensure that the virtual education is not hampered by the disparity of resources. Since the physical classroom learning model cannot be resumed until the universal vaccination of the entire population is not completed in the nation, it should be ensured that technical devices are being made available to every household for the education. This could possibly be done through the way of subsidized prices of the mobiles and other devices. Further, a temporary library could be open in the rural areas with the internet connection available with them, which could consequently help the disabled students in getting the access to the online education without any impediment.

During the time of this pandemic, most of the examinations are taking place through the online mode. The lockdown has posed a peculiar situation in front of the disabled students where they are unable to find out the qualified scribes, readers, or interpreters. Though there is an institutionalized way of getting this facility, however, the challenges posed by the pandemic regarding the dearth of their services are concerning. Therefore, it must be ensured that scribes, readers, or interpreters, are available for the disabled students without any difficulty so that disabled students should face any difficulty in any examination regarding their career.

---

[41] *Id.*

Alternative mediums like radio and television should be utilized extensively for the dissemination of education among the students with disabilities as they are more accessible. The children with disabilities also rely upon the mid day meals for their nutritional development, and this pandemic has stalled the distribution of this meal due to the enforcement of social distancing protocols across the nation. Therefore, it is pertinent for their healthy development that they continue to receive this meal.

## V. CONCLUSION

The current pandemic can wreak havoc to the education of students with disabilities if substantial measures are not being taken for ensuring the inclusive education of these students. Irrecoverable losses would happen if the aforementioned measures are not being taken by the state. Reasonable adjustments in curriculum design, teaching style, and elimination of the paucity of resources would determine the future of students with disabilities. Moreover, content must be made accessible on all video platforms like Webex, Google Meet, etc. so that disabled student does not face any difficulty in accessing learning resources. Subtitles and transcripts of the lectures should be provided along with the recording of the sessions on a regular basis.

In view of the objectives laid down in national education policy, emphasis must be placed on dissemination of knowledge in the mode of vernacular medium so that more and more disabled students can have the benefit of education. Further, all adjustments in education policies should be taken from now onwards keeping in view the interest of students with disabilities. Policymakers should not seeing disabled students as one group as different disabilities require different adjustments to be taken in the policy to cater to their needs. Taking all these measures would not make digital education a distant dream for disabled students, and they would be able to have healthy development in this virtual learning world through proper learning activities.

**BOOK REVIEW**

# UNTIL WE ARE FREE: MY FIGHTS FOR HUMAN RIGHTS IN IRAN BY EBADI SHIRIN

*Rinsha Naraynan**

*"I sound like a dreamer, I know. The challenge facing us today is to think like dreamers but act in a pragmatic manner. Let us remember that many of humanity's accomplishments began as a dream."*

**ABSTRACT**

*In the book titled, Until We Are Free: My Fights for Human Rights in Iran, Ebadi portrays her biography. She clarifies what working in the basic freedom field implies by imparting to us, what she has picked up and lost all through her excursion. The atomic-nuclear settlement with Iran has been reached, and commissions have been lifted. In Iran's ongoing parliamentary political decision, reformists took more seats. To the rest of the world, it might seem like the nation could be nearly going in a different direction. In any case, this is as yet a spot where the individuals who state some unacceptable thing hazard being tossed into isolation, where women are not permitted to work or hold a visa without authorization from their spouses.*

***Keywords:*** *Human Rights, Iran, atomic nuclear settlement, women.*

---

* *III Year, B.BA, LL.B. Student Christ (Deemed to be University), Delhi. The author can be contacted at rinshanarayanano8@gmail.com.*

**BOOK REVIEW**

Ebadi Shirin turned into the primary ever female judge in Iran, in 1975. In any case, after the Iranian Revolution, the new religious ruling classesbashed her out of her position, asserting that Islam restricts a lady to fill in as judge. Though, she was still permitted to provide legal counsel, so she established the *"Defenders of Human Rights Centre*" and spoke to abused women, reporters, activists, maltreated minorities, and numerous other centres of the system's severity and casualties of Iran's degenerate general set of laws. Subsequent to losing her post as ajudge in 1980, Ebadi quit working during the 1980s. It was in the mid-1990s that she began taking generally free cases as a lawyer, shielding children' and women' privileges, a move which prompted the start, she says, of continuous weight and terrorizing concerned her. In 2000 Ebadi was kept in Iran's famous Evin jail for three weeks after a court accused her of "spreading proof of the state's complicity in an assault on understudies the earlier years." The injury of jail brought back Ebadi's youth stammer, which she at last figures out how to defeat after dialectal instruction. Yet, all the badgering just made her more determined. She kept guarding political radicals while getting out the word about them. At the point when Akbar Ganji, an inimitable reformist analytical journalist went on a yearning strike in jail, Tehran's examiner Saeed Mortazavi called his protest unlawful. Thereafter, conversing with journalists, Ebadi alluded to the Islamic Republic respecting the yearning strike of the IRA figure Bobby Sands by naming one of the roads in Iran after him, questioning why outside the nation a craving strike is courageous and daring yet it is taboo inside Iran? As Ebadi sought after her exercises, the waiting game with those in power likewise proceeded. At the point when hardliner Mahmoud Ahmadinejad turned into the president, the Ministry of Education got bolder. It was during that time that Mahmudi, a man in his mid-30s from the service, assumed control over Ebadi's "record" and started to keep a nearby watch on her exercises.

In 2003, she was granted the Nobel Peace Prize, which angered the system.

For quite a long time, she was troubled by the fact that her colleagues, her patrons, family members, and, at last, spouse were regularly tormented and compromised. In this memoir, Ebadi skims over what might be a principal partition in Iranian culture, one that isolates the exclusive classes, from which she hails, from the lower-working classes, which delivered a large portion of her foes. Ebadi left Iran on June 11, 2009, just before the official political decision, to go to a meeting in Mallorca, without realizing this drive would be the start of her being an outcast. As Ahmadinejad got to work for his subsequent term, things got more serious for basic freedoms activists in Iran, including Ebadi who was truly far off. Mahmudi's resentment against Ebadi's exercises was extraordinary to the point that since he was unable to get his hands on her, he turned his displeasure to whoever was close enough and did whatever he could to pound her: keeping Ebadi's significant other and compelling him to give bogus admission on TV against her, pestering her family members and companions, and seizing her things, including her Nobel award and confirmation. The weight was pouring in from all over the place, even from the state charge association which pronounced that the money related honour which Ebadi got alongside her Nobel prize, was available. Subsequently the state put her properties cut-rate. She has most likely that a significant larger part of Iranians needs to see the rear of the system. In any case, she isn't idealistic about the possibilities for change under Iran's present president, the generally moderate Hassan Rouhani, in spite of the fact that she trusts that he may loosen up certain scars on open discussion.

Be that as it may, every one of these endeavours made Ebadi more determined to seek after her movements from outlaw. And this time her crowd isn't just Iran but the world. Equipped with her preparation in both Sharia and common law, and assuming the instances of oppressed correspondents, protesters and minorities, she enters a channel battle inside Iran's falling apart and degenerate general set of laws. Now and again, she can just offer her word world to her readers and their families, analogous to the suspicious death which was ruled a suicide, or the spouse of a reporter

who gradually starves himself to death in jail. Yet, as she talks openly about such cases, she additionally turns into a whistle-blower. Her words advocate for opportunity of articulation, both to Iranians and to the rest of the world.

Ebadi's boldness and quality of character are apparent all through this immersing text, which lights up the drive, few of them had over the many, especially the women and children of Iran. Shirin Ebadi composes of outcast hauntingly and discusses Iran, her country, as the artists do. Ebadi is unafraid of tending to the individual just as the political and does both wildly, with thoughtfulness and fire. I would urge all to read Ebadi's memoir and to see how her battle for basic liberties proceeded in the wake of winning the Nobel Peace Prize. It is additionally entrancing to perceive how she has been influenced decidedly and adversely by her Nobel Prize.

*As the bottom line, the author intends to say that each and every reader should read it and take the lesson that life comes with many challenged but one should overcome it and move forward.*

**BOOK REVIEW**

# ONLINE COURTS AND THE FUTURE OF JUSTICE BY RICHARD SUSSKIND

*Sonam Narayan**

**ABSTRACT**

*Richard Susskind's book, titled, Online courts and the future of justice was written in the year 2019. After the four months of the release of the book worldwide because of the onset of pandemic the book became a reality before the predicted timeline. Richard is of the view that most of the courts have enormous backlog of cases, which indicates that the justice is delayed and in order to sort this issue the online courts might help in achieving the goal. Richard also tries to address the question, is it really essential to have offline court and if not then why not use the digital technology to ensure that the justice is served and made accessible to the common people. The author asks why we can't upgrade our main judiciary to online level. Richard focused that how technology will help us to transform the way justice is delivered. Richard asks readers a very simple question 'Is court a service or a place". Do we really need a court in order to deliver justice?*

***Keywords:*** *Justice, Online Courts, digital technology, order.*

**BOOK REVIEW**

Richard Susskind is the author of the "Online Courts and the Future of Justice". He talks about the need to have an online court in this book.

* *V Year, B.A., LL. B Student, School of Law, University of Petroleum and Energy Studies, Dehradun. The author can be contacted at narayansonam14@gmail.com.*

Professor Richard Susskind OBE is an author, speaker, and independent adviser to major professional firms and to national governments. His main area of expertise is the future of professional service and, in particular, the way in which the IT and the Internet are changing the work of lawyers. The book is published by the Published by Oxford University Press. It was published in the year 2019 and consists of three hundred and sixty-eight pages.

Susskind begins the book by dedicating it to his granddaughter Rosa. He assumed that by the time Rosa, his granddaughter will be 21 in the year 2039 then there is a possibility that there will be more applicability of the technology in the field of the law. But on the contrary the book became the reality in the year 2020 because of the onset of the pandemic. Susskind has divided the book into four parts -

- Courts and Justice (Why courts matter, the case for change, Advances in Technology etc.)
- Is Court a Service or a Place? (The vision, Architecture, Online Guidance etc.)
- The Case Against (Objections, Economy- class justice etc.)
- The Future (Emerging technologies, Artificial Intelligence etc.)

The main argument by the author is that the enormous backlog of cases indicates that the justice is delayed and in order to sort this issue the online courts might help. Richard states that the main objective of the court is to deliver justice and then, the way it is delivered should not play a major role. Richard suspects that in the long run it is the possibility that the justice will be achieved by the AI.

Susskind's work focused on the evolution of the civil dispute in an online forum. He stated that the transition from the traditional to the online court can be firstly achieved by resolving the minor conflict. Once that's achieved then we can focus on the more complicated issue. Susskind talked about the constitutional significance and the jurisprudential function of the judiciary.

One of the most central arguments Susskind gives to incorporate the online courts in the system is that he suggests the reader to do the outcome thinking. He states that sellers do not sell drill; it's the hole which they sell. Similarly, the litigants seek justice and not the judges, courts, lawyers, rules of procedure and etc. Richard do recognizes the fact that ODR exists but he wants the ambit of this ODR to extend from the private to the public sector.

Susskind lays down the complexities of the concept of access to justice. In order to understand the concept in a better manner, author tries to explore what exactly is justice. Susskind discusses the principles of the justice. He suggests that the policy makers while drafting the laws in the context of the online court shall weigh the relevant principles. He states that an accessible, transparent, sufficiently resourced, and a balanced court. Those powers must be backed by the state and the decision and processes should be fair.

The vision laid by the author is that it shall be the justice on which there shall be focus. The physical court shall not be necessary to solve that. In his architecture chapter of the book, author lays down the structure and the hierarchy in which the online court shall be established. Even though as per my opinion that seems quite unreal in the real scenario. Further Susskind introduces the tools to provide the online assessment.

The author tries to answer every possible critic question poised against the online courts. One such example can be the argument that if the courts will go online then how it is guaranteed that the judge will go through all the pages of the documents. Richard states then this issue shall not challenge the competency of the court. The good judges shall be appointed who will fulfil their duties. He suggests that the judge in the case of the online hearing need to be more proactive as compared with the traditional hearing. Suppose, if any part of the evidence is missing then the judges can investigate further and ask for the clarification.

Susskind also further lays down the relationship between the law and the code to lay down the rule for the online court. In his book, he lays down the rules which shall be embedded in the online courts. The rules shall be as such that the layman can assess them. Author also examines the theory of

the online court by referring to the cases where the online court is there in practicality. One such example is in USA in the state of Utah, and the 'e-Courtroom' system in Australia.

The field of AI is very vast but the author has summarized the requisite different conceptions of it in a better manner. He has contended that the AI for the first generation holds a little scope, but he predicts that the second generation will have a wide scope. For the third generation he asks an open ended question to his reader that is it possible that the AI takes over the work of the judges. Susskind ends his book by advising that there needs to be a global effort for adapting the online court system. He is of the view that we need to incorporate an online court system by keeping in consideration the principles of the justice.

As per my opinion the ideas laid down in the book shall be implemented by the judiciary worldwide. The issue of the enormous amount pending cases is something which is being faced by the judiciaries all over the world. One of the core functions of the judiciary is to ensure that the justice is being delivered to the aggrieved. And as the saying goes "Justice delayed is the Justice denied", it is very important to ensure that justice is being delivered timely. As Susskind has very beautifully stated that what matters are the justice and not the fact that from which place it is being delivered. So it is important that now we stop giving the significance to the venue more and rather we shall aim to ensure that the true objective of the judiciary is being achieved.


**Institute of Law**
Nirma University
Sarkhej-Gandhinagar Highway,
Ahmedabad - 382 481. Gujarat, India.
Phone: 079-71652803 / 804 / 815
Fax: +91-2717-241916 / 17
Email: nulawjournal@nirmauni.ac.in