ISSN: 2582 - 2942

LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- V

JUNE 2020

ISSN: 2582 - 2942

DISCLAIMER

ISSN: 2582 - 2942

EDITORIAL BOARD

ISSN: 2582 - 2942

EDITORIAL BOARD

ISSN: 2582 - 2942

ABOUT US

LEXFORTI IS A FREE OPEN ACCESS PEER-REVIEWED JOURNAL, WHICH GIVES INSIGHT UPON BROAD AND DYNAMIC LEGAL ISSUES. THE VERY OBJECTIVE OF THE LEXFORTI IS TO PROVIDE OPEN AND FREE ACCESS TO KNOWLEDGE TO EVERYONE. LEXFORTI IS HIGHLY COMMITTED TO HELPING LAW STUDENTS TO GET THEIR RESEARCH ARTICLES PUBLISHED AND AN AVENUE TO THE ASPIRING STUDENTS, TEACHERS AND SCHOLARS TO MAKE A CONTRIBUTION IN THE LEGAL SPHERE. LEXFORTI REVOLVES AROUND THE FIRMAMENT OF LEGAL ISSUES; CONSISTING OF CORPORATE LAW, FAMILY LAW, CONTRACT LAW, TAXATION, ALTERNATIVE DISPUTE RESOLUTION, IP LAWS, CRIMINAL LAWS AND VARIOUS OTHER CIVIL ISSUES.

The Aarogya Setu Application - A Safety Rose with Legislative Thorns

Aditya Ladha & Samridhi Duggal

INTRODUCTION

The Aarogya Setu application has had a lot of controversies enveloping it since its very inception. Amidst many allegations and legal instructions, the claims of the app being hacked or a major possibility of the data of its users being leaked caused major disruption in the idea of it being a safe app and having all necessary precautions, as claimed by the Indian Government. Furthermore, it is essential to clarify the tenets of an app being suggested v. a mandatory app, which recently caused major stir in a district in Noida.

The app, launched on 10 May, 2020 covering a wide ambit of 11 languages, had already crossed the threshold of 10 million downloads within 5 days of its launch, making its accessibility to a very wide audience. With the usage of the Bluetooth technology and a location-generated social graph, the known usage of the app is to inform a user if he/she happens to cross paths with an individual who has been tested positive. Being available on both servers, i.e. IOS and Android, the app aims to promote social distancing, especially with corona positive individuals.

Before dwelling into the legal aspects of the Aarogya Setu app and the debates that revolve around its provisions and violations as per the Indian laws, it is essential to note how the app works and traces the information.

The Aarogya Setu app detects the presence of the corona virus infection using the GPS system and the Bluetooth technology in smartphones. Via the location, it gives the user information of the history of corona virus cases on the basis of distance. The app also provides for a small corona screening test, including the symptoms, their location and contact history which the users can take on their own and could self-test their possibility of being afflicted by the virus. Additionally, while registering the users are also supposed to also enter any past international travel history, so that it could be traced to the already registered corona cases in the country.

Aarogya Setu was introduced in a pandemic, with a very good intention of the Government to control the spread of corona virus and that beyond the lockdown, general awareness with respect to an Individual's health is given utmost importance. However, this app attracted various concerns that were addressed under the Information Technology Act, 2000, Constitution of India and general principles of fundamental Human Rights. More so, after the Puttaswamy judgment[1], and the

[1]K.S. Puttaswamy & Anr. (Privacy) v. Union of India, (2017) 10 SCC 1

recognition of privacy as a fundamental right, the app infringes varied legal provisions involving the privacy of the citizens of our country.

The paper aims to establish the legal concerns of the app and address the anticipated question of privacy that has consistently been questioned with respect to the Aarogya Setu app with the help of relevant provisions and judicial precedents.

LEGISLATION PERSPECTIVE

Breach of Constitutional Rights

Right to Privacy is the Fundamental Right and is protected by the Constitution.[2] Privacy, as has been described in the famous *Kharak Singh case*[3], is the part or more likely, a subset of the human dignity and personal liberty. When we talk about the human dignity and liberty, the Constitution of India grants these rights to all the citizens of the country under Part III. Every citizen living in this country has the fundamental right to live with personal liberty and dignity and privacy, on the very onset, forms a part of both of these rights. Human Dignity, is not just an aspect of Article 21 (Right to Life and Personal Liberty), but is also well connected with Equality, which is guaranteed under Article 14 (Right to Equality) and freedoms provided under Article 19 of the Constitution of India[4]. Thus, it can be said that when privacy is the subset of the human dignity, it is also linked with all the three fundamental rights, i.e. freedom, liberty and dignity, falling under the combination of Article 14, 19 & 21.[5] There are two approaches that the State can take with respect to the privacy of an individual. The positive approach means that the State takes all the requisite steps to ensure that the privacy of the individual is intact and is not unnecessarily breached upon whereas, the negative approach means that the restriction on intrusion of State over Privacy of an individual.

When we talk about the intrusion of privacy by the State, it needs to be understood that any law or action of the executive breaching such Right needs to fair, just and reasonable. It needs to pass the Test of Proportionality[6]. As per the test, 3 criteria need to be fulfilled:

a. The law or action of the legislative or executive needs to be fair, reasonable and just.
b. The aim of the State in passing such law or action must be legitimate.

---

[2] *Supra* Note 1
[3] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295
[4] K.S. Puttaswamy & Anr. (Aadhar) v. Union of India, (2019) 1 SCC 1
[5] Constitution of India, 1949
[6] *Supra* Note 1

c. The interference should be proportionate to the need.

It must be noted that, when we talk about the law or action passing the abovementioned test, such action or law must also provide a guarantee that there will be no abuse of such interference. The judiciary cannot stop the State on imposing reasonable restriction to the freedom guaranteed under Article 19 as such power is given to them by the Constitution itself. However, it should be kept in mind that such restriction needs to be reasonable.

When we compare the Aarogya Setu Application with the above Constitutional aspects of data privacy, there are many things that need to be noted down. When we see the liability clause of the application, the Terms and Conditions clearly states that the Government will not be liable for the "*inaccurate identification of the infected person*" and the "*inaccuracy of the information*" provided by the in-built server of the Application.[7] This poses a very simple question as to what measures are taken by the Government to stop spreading of fake news.

The Terms and Condition of the app goes on to say that the Government of India will not be liable for any "*unauthorized access*" to the information of the users.[8] When an individual trusts the State with its data, the trust develops on the very foundation that the data provided by him/her will be safe and will not be used for any illegitimate purpose. Data privacy and protection needs to be ensured at every step of such a big project.[9] By adding on to this clause, it creates a suspicion in the mind of the users with respect to the data protection. Though there is a clause of Privacy Policy in the Application, which talks about the data encryption[10], it needs to be noted that it is nothing except the weak assurance to the public that the data is safe. In reality, the encryption does nothing to do away with the privacy issue.

Though the app suggests that the information of the application will be used by the Government in anonymized, aggregated manner for the purpose of generating reports and heat maps[11], it also says that the data will be shared with "*other necessary and relevant persons*" for "*necessary medical and*

[7]Clause 6(c), Limitation of Liability, Terms of Service, Aarogya Setu Application, available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.
[8]Clause 6(d), Limitation of Liability, Terms of Service, Aarogya Setu Application, available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.
[9]*Supra* Note 4
[10]Clause 5, Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.
[11]Clause 1(a), Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.

administrative intervention"[12], which depicts that the data can be subject to the inter-departmental exchanges. The policy is not at all clear as to who these other necessary and relevant personnel are and what all is included in the term administrative intervention. Also, though the applications privacy policy suggest that the data will not be disclosed to any 3rd party[13], a co-joint reading of the clause 1(b) tells that the information of one user is securely placed in the mobile device of the other user when they come in contact with each other, while the Bluetooth is on. This, however, puts the data of the users at risk as there are chances that the other person, with enough technical knowledge and know-how, might implant bugs and viruses in the mobile device of the user. Thus, this clearly violates the Right to Privacy under Article 19 and 21 of the Constitution of India.

As per the recent news reports, the Central Government mandated the use of Aarogya Setu Application for both the public as well as private sector workers, during the third phase of lockdown, which was implemented from May 1st, 2020 to May 17th, 2020[14]. Though, during the 4th phase of the lockdown, the mandatory clause regarding the usage of the application was changed to the Advisory clause of usage[15], still there are millions who registered themselves on this application. Thus, it becomes important to discuss the breach of Constitutional Rights of those individuals, who registered themselves on the application solely due to its "*mandatory clause*". As per the Terms of Use of the app, the terms of the application are subject to continuous amendment and failure to comply with any of these amendments will lead to restriction to use the app.[16] A co-joint reading of the above lines show that once the use of the app is mandated, the user will be forced to give consent to the terms and conditions, which in turn can hamper the privacy of the user and is therefore, unconstitutional as it takes away the Right to Consent from the individual, which have been granted to him under Article 21 of the Constitution of India.[17]

---

[12]Clause 6, Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.
[13]*Ibid.*
[14]*Coronavirus Pandemic | Aarogya Setu app mandatory for govt, private sector employees*, available at https://www.moneycontrol.com/news/india/coronavirus-pandemic-arogya-setu-app-mandatory-for-govt-private-sector-employees-5213901.html, last accessed on 17/05/2020 at 10:25 a.m.
[15]*Aarogya Setu: MHA dilutes Mandatory imposition; says employer on 'Best Effort Basis' should ensure Use of App by employees with 'Compatble Mobile Phones'* available at https://www.livelaw.in/top-stories/aarogya-setu-mha-dilutes-mandatory-imposition-156921, last accessed on 20/05/2020 at 03:36 p.m.
[16]Terms of Use, Aarogya Setu Application, available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.
[17]*Supra* Note 1

The privacy policy states that, "*all the personal information collected under clauses 1(b), 1(c) and 1(d) will be retained on the mobile device for a period of 30 days from the date of collection, if it has not been uploaded on the server.*"[18] Now, when any user of any application uninstalls that particular application, it is deemed that such user withdraws the consent already given to the Terms and Conditions of such application. In the present case, even after the uninstallation, which means withdrawal of the already given consent, the data will be present[19] in the mobile device of the third party, without the consent of the user, violating the Right to Consent, provided under Article 21 of the Constitution.[20]

The above issues in the app do not pass the test of proportionality as it does not guarantee that there will be no data leakage. Along with that, the presence of data of the user on the mobile device, even after uninstalling the application, violates the 3rd point of test, where the extent of interference is more than required. There are no proper safeguards along with the application that ensures that in no case there is a threat to the data of the individual. Thus, it can be said that mandating the use of Aarogya Setu application in the public and private sector violates the Fundamental Right of Privacy, which is enshrined by the combination of Article 14, 19 and 21 of the Constitution of India, and is thus, unconstitutional.

The Supreme Court held that the apprehension is mere fear or anxiety of something happening. A policy or law or action of the executive cannot be shelved merely on the grounds of apprehension, if it caters to the larger social interest and outweighs the personal claim of privacy.[21] Thus, it can be said that if the State ensures that there will be no data leakage, a law by the legislation or action of the executive, along with the reasonable restrictions, can be passed and stands valid.

Information Technology (IT) Law violations

During a webinar organized by an advocacy group, Former SC Judge, Justice Srikrishna revealed his concerns with the use of Aarogya Setu application, which was made mandatory by the Central Government, for the employees of public sector as well as private sector, during the third phase of lockdown (i.e., 03rd May, 2020 to 17th May, 2020). He said that the mandatory use of this app causes

[18]Clause 3(b), Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.
[19]Clause 4(b), Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.
[20]*Supra* Note 1
[21]*Supra* Note 4

more concern in the minds of people, as opposed to the benefits.[22] Justice Srikrishna, the head of the Srikrishna Committee, which proposed the Draft Personal Data Protection Bill, 2018, is considered to be a pioneer in the data protection and privacy laws. Though the Bill is still pending in the Parliament, awaiting the assent of both the houses, to be enacted and enforced as an Act, it aims at improving the Data Protection laws and monitoring the surveillance in India.

When we talk about the data privacy and protection, there are several aspects in the IT Law as well which gets violated on mandating the use of Aarogya Setu application. These violations not only concerns with the processing of the data collected, but also raises serious questions with respect to the retention of data so collected, even after the application has been uninstalled from the smartphone of the registered user. For the purpose of the same, the researchers, in this paper will be analyzing the IT Act[23] and the Personal Data Protection Bill, 2018[24] and look upon the provisions, which gets violated with the use of the application being mandated.

Information Technology Act, 2000

As per the definitions given under Section 2 of the Information Technology Act (hereinafter, IT Act, 2000), the *intermediaries*, in reference to the electronic records, have been defined as anyone, who himself or on behalf of someone else, stores or transmits the electronic records mentioned above or provides any service with respect to the mentioned records.[25] The intermediaries include several key players such as telecom service providers, web hosting service providers, cyber cafes, etc.[26] When one analyzes the definition given above, the mobile application service providers also tend to fall in the definition of intermediaries. The mobile applications, as per Mr. Salman Waris, Partner at Tech Legis Advocates and Solicitors, thus fall under the ambit of intermediaries as per IT Act, 2000.[27]

The IT Act also contains the provision with respect to the compensation in case there is a failure to protect the data so provided by any individual.[28]As per Section 43A, in case the body corporate fails

---

[22] *"It causes more concern to citizens than benefits": Justice B.N. Srikrishna says, "Mandating the use of Aarogya Setu app is utterly illegal"* by Akshita Saxena, on 12/05/2020 at 01:48 p.m., available at https://www.livelaw.in/top-stories/justice-bn-srikrishna-says-mandating-the-use-of-arogya-setu-app-is-utterly-illegalwatch-video-156629, last accessed on 20/05/2020 at 04:24 p.m.

[23] Information Technology Act, 2000

[24] Bill No. 373 of 2019

[25] Section 2(w) of the IT Act, 2000

[26] *Ibid*

[27] *Legal Experts point out the liability concerns with the Aarogya Setu App*, by Anandi Chandrashekhar and Surabhi Agarwal, The Economic Times, available at https://economictimes.indiatimes.com/tech/software/legal-experts-point-out-liability-concerns-with-the-aarogya-setu-app/articleshow/75561944.cms, last accessed on 20/05/2020 at 04:53 p.m.

[28] Section 43A of the IT Act, 2000

to protect the sensitive personal data or the information so possessed by it, and is negligent in implementing the reasonable security measures, which consequently results in a wrongful gain or loss, the body corporate is held liable to pay the damages to the affected person, by way of damages.

Now, when we look at the Liability Clause of the Aarogya Setu application, it clearly states that the Government of India will not be held liable for any unauthorized access to the data of the registered users.[29] When Section 2(w) and Section 43A of the IT Act are co-jointly read, it becomes very clear that the intermediary, in this case, the Aarogya Setu App (services provided by NIC, which comes under the Government of India[30]), will be held liable in case of data breach or mishandling of the data of the individual. Thus, Clause 6(d) of the Terms of Service of the application is the clear violation of Section 43A of the IT Act, 2000.

IT Act, 2000 also provides that the intermediaries can be exempted from the liability in certain cases.[31] However, looking at the pre-conditions, it becomes certain that the Aarogya Setu App does not fall under this category as it says that the intermediary is not liable when a third party data or communication is made available or hosted by it. It also says that in order to be exempted from the liability, the intermediary needs to observe due diligence while discharging its duties.[32] The duties of the intermediary also involve its duty to not disclose any personal information, which have been provided in terms of contract, as under Section 72A of the IT Act, 2000.[33] It has been held by the Delhi High Court that the presence of any active participation by the intermediary can take away their protection present under the exemption of liabilities.[34] Thus, in the present scenario, even if the Government of India tries to evade their liability in case of unauthorized access to the personal data of the users[35], it cannot do so as it does not fall under the protection provided by the IT Act, 2000[36], where certain intermediaries are exempted from the liability.

Personal Data Protection Bill, 2019

[29]Clause 6(d), Limitation of Liability, Terms of Service, Aarogya Setu Application, available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.
[30]As per the details of the application given in the Google Play Store
[31]Section 79 of the IT Act, 2000
[32]Section 79(2)(c) of the IT Act, 2000
[33]Shreya Singhal v. Union of India, (2015) 5 SCC 1
[34]Christian Louboutin Sas v. Nakul Bajaj, (2018) 253 DLT 728
[35]*Supra* Note 7
[36]*Supra* Note 31

In order to lay down a global digital landscape in this highly digitalized era, it is much needed that a proper legal framework should be laid down by India[37] and to serve this purpose, the Personal Data Protection Bill was formulated. Further, the need was also felt after the famous *K.S. Puttaswamy* judgment[38], in which the Right to Privacy was considered as a Fundamental Right. The Directive Principle of State Policy, as mentioned in the Constitution of India, also holds that it is the duty of the State to lay down laws, which serves for the common good of the people.[39] Thus, it becomes very important to analyze the Aarogya Setu application with respect to the Personal Data Protection Bill, 2019 (Hereinafter, the Bill) as it is the first dedicated legislative framework, with respect to the Data Protection, in India.

As per the Bill, the person or the individual, to whom the data relates, is said to be the *Data Principal.*[40] When any person, which also includes the State, who in conjunction with others or alone, process the data of the Data Principal or determines the means to process such data, is known to be the *Data Fiduciary.*[41] Thus, in the present scenario, the individuals downloading the Aarogya Setu application are the Data Principal and the State (Government of India), the Data Fiduciary.

When it comes to defining the Personal Data of the individual, it can be defined as any data, which is related to the individual and such individual can be directly or indirectly identified with the help of such available data.[42] Any accidental or unauthorized disclosure, use or alteration to such personal data, which subsequently compromises the confidentiality of the Data Principal, is defined as a Breach of Personal Data under the Bill.[43] Now as far as the Personal Data is concerned, certain aspects of the Personal Data has been further classified as the Sensitive Personal Data in the Bill. The Sensitive Personal data also includes the health data of Data Principal. Therefore, applying the abovementioned definitions in the present scenario, any breach of data, of the registered users, in the Aarogya Setu application, shall be considered as the Breach of Sensitive Personal Data and the handler of such data, in the present case the Government of India, will be held liable under Section 43A of the IT Act, 2000. Further, the Bill also holds the Data Fiduciary responsible for any processing of data, either undertaken by the Data fiduciary itself or on its behalf.[44] Thus, by mere

[37] *A Free and Fair Digital Economy, Protecting Privacy and Empowering Indians:* Justice B.N. Srikrishna Committee Report
[38] *Supra* Note 1
[39] Part IV, Constitution of India, 1949
[40] Section 2(14) of the Personal Data Protection Bill, 2019
[41] Section 2(13) of the Personal Data Protection Bill, 2019
[42] Section 2(28) of the Personal Data Protection Bill, 2019
[43] Section 2(29) of the Personal Data Protection Bill, 2019
[44] Section 10 of the Personal Data Protection Bill, 2019

insertion of the Liability Clause stating that the Government of India will not be liable for any unauthorized access[45], cannot help the Government in evading the liability and thus the compensation has to be paid to the Data Principal in case of such breach.

Moving towards the provision regarding the retention of data in the Bill, it clearly states that the Data Fiduciary shall not retain the data of the Data Principal for a longer period, unless explicitly consented to by the Data Principal or is deemed necessary as an obligation under any law during that time.[46] Further, the Data Principal has the right to the erasure of Personal Data, when such data is no longer needed for the purpose of which it was processed in the first place.[47] When the data is approved for erasure, the Data Fiduciary shall notify all the relevant authorities, with whom such data was shared initially.[48] When we look at the Privacy Policy of the Aarogya Setu Application, it clearly states that all the information collected from the user at the time of registration, will be retained as long as the account on the application remains in existence[49], which is a clear violation of the above mentioned provisions of the Bill.[50] Similarly, there is no where mentioned in the application as to what will be done with the data, once the user uninstalls the application and why the data will be retained by the Data Fiduciary for a period of 30 days.[51] Further, it is pertinent to note that nothing has been mentioned with respect to the data shared with the "*relevant authorities*"[52], in case, the user exercises his Right to erasure of the registered data under the Bill.[53]

Though the application violates many provisions of the IT Law, it must be noted that the anonymization of data of the individuals is the clause in the Terms of Use of the Application, which clearly goes hand in hand with the Personal Data Protection Bill, 2019. Thus, there are so many loopholes which ought to be considered, in order to do away with the concerns regarding the Data Protection and Data Privacy of the registered users.

Human Rights Violations

[45] *Supra* Note 8
[46] Section 9(2) of the Personal Data Protection Bill, 2019
[47] Section 18(1)(d) of the Personal Data Protection Bill, 2019
[48] Section 18(4) of the Personal Data Protection Bill, 2019
[49] Clause 3(a), Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.
[50] *Supra* Note 47
[51] *Supra* Note 19
[52] *Supra* Note 12
[53] *Supra* Note 48

Right to privacy has been enshrined in the International Treaties and Covenants from the very beginning. This right is identified as the basic human right, which should be available to the individuals, by the virtue of being a human being at the very instance. When we talk about the Universal Declaration of Human Rights (hereinafter UDHR) and the International Covenant on Civil and Political Rights (hereinafter ICCPR), both the Covenants recognize the Right to Privacy not only as a basic, but special Human Right, violation of which can cause legal repercussions.

UDHR states that the no individual shall be subject to any arbitrary interference, when it comes to his privacy.[54] Similarly, the ICCPR holds that in case the Right to Privacy of an individual has been interfered with arbitrarily, the individual can seek remedy under law against such interference.[55] It also holds that in case the data so been collected have been collected or processed wrongly or against the provisions of law, the concerned individual has the Right to request immediate elimination or rectification of such data.[56] In 2013, the United Nations General Assembly, in a resolution, mentioned the requirement that the Government, while collecting or processing the data of the individual, must comply with their obligation with respect to the security of the public data and such compliance shall be in accordance to the International Human Rights regime.[57] It should be noted that India is signatory to the above mentioned Treaties and the Covenants and thus, under the DPSPs provided in the Constitution, it is required to respect and uphold the obligations under the international law.[58]

The controversy, which stirred with the argument of Senior Advocate Mukul Rohatagi, that the Indians do not have the Right to Privacy as a Fundamental Right, forced the Supreme Court to answer the issue, which was need of the hour. The Supreme Court, with respect to the inalienability of the Right to Privacy, held that the Right to Privacy is available to an individual from the very instance of him being a human being and thus, when such Right is read in consonance with Article 21[59], it becomes very clear that such a right is inalienable and thus, cannot be taken away from the individual.

---

[54]Article 12 of the Universal Declaration of Human Rights
[55]Article 17 of the International Covenant on Civil and Political Rights
[56]General Comment No. 16 to Article 17 of the International Covenant on Civil and Political Rights
[57]*The Right to Privacy in Digital Age*, General Assembly Resolution No. 68/167, adopted on 18/12/2013, available at https://undocs.org/pdf?symbol=en/a/res/68/167, last accessed on 24/05/2020 at 05:43 p.m.
[58]*Supra* Note 5, Article 51
[59]*Supra* Note 5

When the use of the application was mandatory by the Central Government during the 3rd phase of the lockdown, it can be said as the forceful interference within the ambit of a person's privacy, and the constant surveillance by the way of application being mandated was a serious threat to an individual's freedom of movement[60] and right to life & liberty[61]. Though the app has been developed with the intention to help the people of India in these tough times of pandemic, the lack of transparency on the part of Government on previous instances causes suspicion in minds of people.[62] Thus, the application causes serious human rights violation.

GOVERNMENT'S LIABILITY

Data breaches and leakages have been common news since the internet technologies have escalated their prospects. With the changing dynamics of the Aarogya Setu application from being mandatory to an optional precaution, understanding the liability of the Government with respect to the usage and in a prospective leak of data is essential public knowledge.

The Questions of the liability of the Government were brought forward by legal experts when it was made compulsory during the third phase of the lockdown.[63] Claimed to have been developed with the best internet practices, the tweet regarding security concerns by a French Hacker, hustled the questions on the privacy policies of the Application even more.

According to the Terms and Conditions of the App[64], it is stated that the "*users acknowledge and agree that the Government of India will not be liable for any unauthorized access to your information or modification thereof*"[65] This clause is generally used to indemnify companies and institutions, and in this case aims to indemnify the Government in case of an unauthorized access to the personal information of its users. Conveniently enough, this clause also aims to protect the Government of any future liability that may arise in a case of data breach of any sort, irrespective of the Government being responsible for the introduction of the application and witnessing millions of downloads on a daily basis.

---

[60] Article 13(1) of the Universal Declaration of Human Rights

[61] *Supra* Note 5, Article 21

[62] *Would Narendra Modi please care to answer some questions about PM-Cares?,* Manoj Harit, available at https://thewire.in/government/pm-cares-covid-19-fund-narendra-modi, last accessed on 24/05/2020 at 06:00 p.m.

[63] *Aarogya Setu app mandatory: Who all must download the app right away*, Techdesk, The Indian Express, available at https://indianexpress.com/article/technology/social/aarogya-setu-app-mandatory-contact-tracing-app-6389284/, last accessed on 17/05/2020 at 12:30 p.m.

[64] Clause 7, Terms of Service, Aarogya Setu Application, available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.

[65] *Legal experts point out liability concerns with the Aarogya Setu app*, Anandi Chandrashekhar and Surabhi Agarwal, available at https://economictimes.indiatimes.com/tech/software/legal-experts-point-out-liability-concerns-with-the-aarogya-setu-app/articleshow/75561944.cms?from=mdr, last accessed on 23/05/2020 at 01:00 p.m.

The National Informatics Centre (NIC), being the application service provider owes to its credit, the development and encryption of the Aarogya Setu Application. The application requires the users to insert their personal and private information[66] on to the NIC server, which then enables this contact tracking device to function properly. NIC, under the Government Ministry of Electronics and Information Technology falls under the definition of an "intermediary"[67] as per the IT Act, 2000. Even under clause 2(13) of the proposed Personal Data Protection Bill, 2019[68] the Government of India is a data fiduciary and has to necessarily comply with the obligations of data privacy set out for them.[69] The summary of the aforementioned references is that the NIC, being the intermediary in this case is obligated to ensure the security of the data collected and shall be held liable for the loss of it under the intermediary guidelines.[70] The same was also upheld by the Delhi High Court, where it clearly establishes the principle that if an intermediary plays a direct role in the disputed disposition, it shall be held accountable for any breach.[71] Holding NIC accountable would automatically make the Government also liable for such data leakage, as it falls under the ambit of the Government and its activities.[72] The same logic is also legally supported by Section 43A of the IT Act[73], wherein it is stated that anybody dealing with the sensitive personal data fails to comply with the privacy norms shall be liable and bound to pay adequate damages, which in this case, is the NIC backed by the Government of India.

We cannot aim to properly dwell into the liability of the Government without a proper analysis of the privacy policy encapsulated in the Aarogya Setu application. The application is based out of the *purpose limitation* principle.[74] This principle recorded under Article 5(1)(b) of the GDPR aims on a

[66]The nature of the personal information provided in the application, complies adequately with the definition provided under Section 2(1)(i), Information Technology (Reasonable Security Practices and Procedures and Sensitive personal data or information) Rules, 2011
[67]*Supra* Note 25
[68]*Supra* Note 41
[69]*Data Privacy & Aarogya Setu Covid-19 app,* Rupali Bandhopadhya and Arun Gupta, available at https://timesofindia.indiatimes.com/blogs/voices/data-privacy-aarogya-setu-covid-19-app/, last accessed on 23/05/2020 at 2:30 p.m.
[70]*Supra* Note 34
[71]*Ibid*
[72]Section 67C, Information Technology Act, 2000
[73]*Supra* Note 28
[74]Clause 2(a), Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.

general underlying base that the data collected by any source for a specific purpose should not be used for any other purpose.[75]

In this case, the data being collected by the application is ideally limited to the identification and reduction of the Covid-19 disease. Key highlights of the privacy policy of the application are as follows:

1. The personal data should be used only for generating reports, heat maps, and other statistical analogies for the purpose of management of Covid-19 in the country.[76]
2. It is claimed that the app is equipped with standard security features.[77]
3. It is specifically mentioned that the data would not be disclosed or transferred to any third party under any circumstances[78] and a data retention limit between 30-60 days is also stipulated in the application.[79]

In simpler terms, the data that is recorded via the medium of this app, should not be used for any other purpose beyond the extent of Covid-19. Interestingly, branched out in the lieu of a pandemic and with specific limitations and restrictions, the terms and conditions and the privacy policy of the application contradict each other at a fundamental level, which even, to some extent defies the purpose of limitation principle. Clause 4 states[80] that while the users tap the "I agree" option while downloading the app, they consent to the collection and use of their personal data and can revoke the usage of the same via switching off the Bluetooth option or uninstalling the application from their smartphones. However, clause 3[81] states that even post the cancellation of one's registration, the data shall remain on the server for a period of 30 days, in case of a non-positive user, 45 days for a tested positive, but cured user and a reasonable time, on a "case-to-case" basis. Consent has always been a very subjective term in our legal dictionary, but to simplify it, does uninstalling the application from my personal device not amount to a withdrawal of consent? When the permission

---

[75]*Chapter 6: Data Protection Principles – Unlocking the EU General Data Protection Regulations*, available at https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection, last accessed on 24/05/2020 at 2:30 p.m.

[76]*Supra* Note 74

[77]The word, claimed, is written herein because nowhere in the privacy policy have these *standard features of protection and security been* mentioned or specified. Moreover, the adapted encrypted security mechanisms have also not been mentioned in the privacy policy of the app.

[78]*Supra* Note 12

[79]Clause 3, Privacy Policy, Aarogya Setu Application, available at https://static.swaraksha.gov.in/privacy/, last accessed on 17/05/2020 at 01:00 p.m.

[80]Clause 4, Terms of Service, Aarogya Setu Application, available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.

[81]*Supra* Note 79

to use the inserted data is withdrawn by the user, how is its usage and rotate is not an invasion of the user's privacy, which, as already adjudged is a fundamental right of all citizens of our country.

A common thing in most of the telecasted debates is how the people are comparing this Aarogya Setu application to the Aadhar Case. One of the arguments brought up during the pleadings was how Indians did not have the fundamental right to privacy. The Puttaswamy Judgment, in pure culmination addressed the question and stated that "*it is only the ability of an individual to protect a zone of privacy, which enables a complete realization of the full value of life and liberty.*"[82]Additionally, Clause 6[83] addresses the "liability" tangent of the application and states that the Government shall not be liable for a failure of the app or the accuracy of the information so provided. Moreover, determining an individual's geographical location, name, phone number are all mostly the personal data of the individuals, asking for which, cannot be made mandatory, nor can it be dealt with carelessly with a no-liability clause making a clear cut escape for any breach or mishandling of stored data.

The General Public might be confused with the perception, that the Aarogya Setu Application is a product of the Information Technology Act, however, since this application was drafted for and introduced during a pandemic, it is developed under the wide umbrella of the Indian Disaster Management Act. It must also be noted that the Indian *Disaster Management Act*[84]allows adequate measures and data collections via the Government in order to prevent disasters. Covid- 19, as a pandemic easily passes as a disaster and the introduction of Aarogya Setu, with the intention to control this pandemic affirms with the long term goals of the Government.

In correspondence with the abovementioned data collection, it must also be kept in mind that the violation of fundamental rights cannot be accepted via any medium is a judicial perception, which lays one of the tombstones of our faith and belief in the Indian Judicial System. Via the virtue of the 44th Constitutional Amendment[85] and the reversal of the erroneous judgment delivered in the ADM Jabalpur Case[86], it is very clear that fundamental rights of the citizens cannot be done away with and the Disaster Management Act is no exception to this. Part III of the Constitution explicitly states that the justification of a violation of our fundamental rights necessarily requires an existing law

[82]*Supra* Note 1
[83]Clause 6, Terms of Service, Aarogya Setu Application , available at https://static.swaraksha.gov.in/tnc/, last accessed on 17/05/2020 at 12:45 p.m.
[84]Section 36 of the Disaster Management Act, 2005
[85]The 44th Constitutional Amendment, 1978
[86]ADM Jabalpur v. Shivkant Shukla (1976) 2 SCC 521

authorizing the same.[87] The NDMA cannot be this existing law in the current pandemic, because it fails to lay down a basic structure of varied circumstances, limitations and execution models. If the NDMA is accepted as the law that can indeed, be accountable for violating the privacy of the citizens, the Government, in a hypothetical situation, can do absolutely anything in the situation of a disaster and India would be facing another Emergency situation.[88]

The legal requirement of introduction and implementation of the application, even though falls clearly under the wide ambit of the powers granted to the National Disaster Management Authority[89], however, it still fails to stand clear on the tests of need and proportionality.[90] Is there a need to invade the privacy of the users? Or is controlling the corona pandemic equally proportionate to risking the personal data of millions of users while making it mandatory are questions that need to be addressed via a legislative mindset. The Aadhaar Judgment highlights also the fact that beyond the test of proportionality, if a breach of privacy, or any fundamental right is witnessed, the onus to disprove the same lies on the State. Similarly, if the Government claims that there is no invasion of privacy and that there would not ideally be a data breach, they should prove it with legislature, how the violation is non-existent and the liability in case of a future data misuse.

While addressing the question of liability of the application, the two things that must be kept in mind are that the application involves the usage and processing of private and even sensitive personal data[91] and since the application has been made in lieu of a pandemic and not directly under the IT Act, invoking Sections 43A and 72 in order to prove the liability and probable damages for the same may not be considered as reasonable best options.[92] It can also be argued that the challenged disclosure was made under the regulation or subjected to prior approval[93], however, the same does not exempt the liability of the Government in case of withdrawn consent or breach of personal sensitive data. Hence concluding, that even though the application was not made under the IT Act, the DMA is not a competent legislation to adjudicate the matters coming on this pretext,

---

[87]Part III of the Constitution of India, 1949

[88] Reference to the Emergency that was declared by our late prime minister, Mrs. Indira Gandhi, from 25 June, 1975 till 21 March, 1977

[89]Section 6(2)(i), The Disaster Management Act, 2005

[90]In the Puttaswamy Judgment, a clear threefold standard testing procedure was established, which laid down the tenets of invasion of privacy by the Government. The test was that of, Legality, Need and Proportionality.

[91]Section 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[92]*Misuse of Aarogya Setu Data: Addressing the question of liability,* Kunal Kishore Bilaney, available at https://thelawblog.in/2020/05/09/misuse-of-aarogya-setu-data-addressing-the-question-of-liability/, last accessed on 24/05/2020 at 07:20 p.m.

[93]Awadhesh Kumar Paras Nath Pathak v. State of Maharashtra & Anr. [Cr. App. No. 2562 of 2019]

such as data leakage or breach of the stored and deposited data, hence the IT Act is capable of administering the same and addressing all claims of liability and damages.

When the application was made mandatory during the 3rd phase of the lockdown or even when it was presented as an advisory during the 4th phase of Lockdown, the question of the Government's liability in a prospective case of data breach cannot be addressed in terms of black and white. The clash of human life versus the fundamental rights that make a human life worth it essentially lies on the concept of interdependence. The Government's steps to control the pandemic and save India from a situation that is beyond our predicament, is laudable however, the application that aims to serve as a tool to control this pandemic is legally flawed and despite best intentions, in case of an infringement or breach, the Government of India should ideally be held accountable for the same. In accordance with the research analyzed above, it can be concluded that the Government does owe a liability and the no-liability clause in the privacy policy of the application does not indemnify it against its responsibilities. However, the extent of the Government's liability cannot be predicted and is awaited via a proper legislative analysis.

INTERNATIONAL PERSPECTIVE

While the Aarogya Setu application is prevalent in India, there are other countries as well, who are using the similar applications in an effort to minimize the effect of Covid-19, in their respective countries. However, there has been a split between the types of apps that the countries are using. There are two models of apps, the centralized version and the decentralized version. The centralized version holds the gathered data in the centralized server, whereas in the decentralized version, keeps the data on the user's phones and it is on their phone, that the matches are made if one comes in contact with the Covid-19 patients. However, it is pertinent to mention that both of these applications use the Bluetooth signals of the smartphone.[94]

Countries like UK, India, Norway, etc. use the centralized model of the application. This gives the authorities an insight into the data of the registered users, which in turn risks the privacy of the individuals. However, there are countries like South Korea as well, which has not used the concept of contact tracing and has still managed to flatten the Covid-19 curve. However, the surveillance system in South Korea worked a bit differently, and during the initial times, the Government release

[94] *Coronavirus contact-tracing: World split between two types of apps*, Cristina Criddle and Leo Kelion, available at https://www.bbc.com/news/technology-52355028, last accessed on 24/05/2020 at 10:30 p.m.

too much of data, and thus, it resulted into revealing the identity of the patients, who subsequently got harassed.[95]

The decentralized model of the application has been developed by Apple and Google together.[96] However there has been a problem in the contact tracing due to the restriction on the use of Bluetooth by Apple in the iPhone.

A table has been displayed on the website of *The Hindu*, which has used several grounds to evaluate the contact tracing applications, used worldwide, by different governments,[97] such as transparency, mandatory installation, etc. The table shows that the countries like China, Turkey and India raises concerns with respect to the data privacy because the answer to at least three above mentioned grounds is NO. Thus, the data privacy of several individuals being at risk is a serious concern worldwide and it the issue is of utmost important, and therefore, needs to be answered urgently, along with relevant rectifications.

AUTHORS' NOTE

The authors, via this Research Paper nowhere discredit the efforts of the Government to minimize and control the pandemic. It deeply addresses the anchors of legislative flaws in the Application and seeks to look forward to a legalized redressal system and a prepared mechanism in case of a data breach. Upholding the principles of transparency, the validation of Constitutional Fundamental Rights and democracy in general lay the foundation of our judicial system.

The Aarogya Setu Application, which is drafted on the broken limb of NDMA fails to bear the review of the honest test of proportionality and the onus to prove the authenticity and legality of the same, falls on the shoulders of the Government. An invasion or threat to privacy is a serious question that must be calculated and judicially supported, even during a pandemic.

The application, when read with the Puttaswamy judgment, should have been legally backed by a specific law. With least infringement, it should have been proportionate to the sought objective. The

[95] *Coronavirus contact tracing app means spying, end to data privacy*, Bloomberg opinion, available at https://www.deccanherald.com/opinion/coronavirus-contact-tracing-apps-mean-spying-end-to-data-privacy-835786.html, last accessed on 24/05/2020 at 10:47 p.m.

[96] *The Apple Google contact tracing system won't work. It still deserves a praise.*, Jennifer Daskal & Matt Perault, available at https://slate.com/technology/2020/05/apple-google-contact-tracing-app-privacy.html, last accessed on 24/05/2020 at 10:50 p.m.

[97] *Data | How safe is Aarogya Setu compared to Covid-19 contact tracing apps of other countries?*, The Hindu Data Team, available at https://www.thehindu.com/data/how-safe-is-aarogya-setu-compared-to-contact-tracing-apps-of-other-countries/article31618852.ece, last accessed on 24/05/2020 at 11:00 p.m.

questions of is the invasion of the user's privacy absolutely necessary to control the Covid Disease and which redressal form do the users approach in case of a breach are stranded on the shreds of the Government's shoulder, which need to be answered via a capable legislation or amended clauses.

Despite commendable efforts of the Central Government, the questions of liability and accountability must be addressed effectively. While addressing the concerns under the Constitution, IT Act, and general principles of human law, having a more transparent approach, exemption/amendment of the no-liability clause and full disclosure of the security, encryption features as may be deemed fit can be some of the steps to address this invasion and maintain a stable control of fundamental rights and the pandemic. With high hopes with the Petition pending in the Kerala high court, it is concluded, that despite being a great leap for safety and prevention, the application needs to address the elephant in the room and establish a system where there is least intrusion and no violations, while also addressing that the creators and promoters of the application shall be accountable for a breach of their sensitive personal data.

BIBLIOGRAPHY

1. Statutes

a) Constitution of India, 1949
b) IT Act, 2000
c) Personal Data Protection Bill, 2019
d) Universal Declaration of Human Rights
e) International Covenant on Civil and Political Rights
f) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
g) National Disaster Management Act, 2005

2. Judicial Precedents

a) K.S. Puttaswamy & Anr. (Privacy) v. Union of India, (2017) 10 SCC 1
b) K.S. Puttaswamy & Anr. (Aadhar) v. Union of India, (2019) 1 SCC 1
c) Shreya Singhal v. Union of India, (2015) 5 SCC 1
d) Christian Louboutin Sas v. Nakul Bajaj, (2018) 253 DLT 728
e) ADM Jabalpur v. Shivakant Shukla, (1976) 2 SCC 521
f) Awadesh kumar Paras Nath Pathak v. State of Maharashtra, Cr. Appl. No. 2562 of 2019

3. Online News Websites and Blogs

a) timesofindia.com
b) thewire.in
c) moneycontrol.com
d) bbc.com
e) livelaw.in
f) deccanherald.com
g) economictimes.com
h) whitecase.com

4. Resolutions and Committee Report

a) Justice B.N. Srikrishna Committee Report on Draft Personal Data Protection Bill, 2019
b) General Assembly Resolution No. 68/167