

---

**INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH**

---

**AN ANALYSIS OF RIGHT TO PRIVACY**- Arunim Kathuria & Radhika Mittal<sup>1</sup>**Abstract**

Privacy is one of the most essential and basic call in a person's life. It is that pre requisite which is indispensable in nature. Everyone has inherent right to enjoy their privacy be it at their home or in public. Privacy is something which is as ancient as this human race and as contemporary as this changing society. It is something which is deeply related to human integrity, personal liberty and autonomy to enjoy freedom. The importance of privacy can be seen in our day-to-day life but due to rapid advancement in technology it is becoming more and more challenging to safeguard our privacy. Despite such cumbersome route, judiciary has always tried to play its role effectively and efficiently. It has paved the way and brought this concept as a matter of right under Article 21 of the Constitution of India by judicial activism. The aim of the study is to bring about a deep analysis of the concept of privacy, the jurisprudence of historical development of privacy leading upto fundamental right in the law of the land and to present the current scenario of privacy in this Covid-era. The paper, firstly, discusses the law of privacy as a whole built up by different statute. It tried to show linkage of privacy with different aspects of life and how it attained a constitutional status. Secondly, the paper brings in picture, the position of right to privacy in different countries and how it was incorporated in those countries. It tried to bring in light the pros and cons of internet privacy which is the most vulnerable area of today's world. This paper is an exhaust study of the concept of privacy with landmark judgments. It also discusses the penal provisions given in different statute for violating privacy.

---

<sup>1</sup> Students at JIMS, Greater Noida

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

## INTRODUCTION

In the layman language, privacy may be understood as being in a state of isolation or in simple words, privacy mean seclusion. According to Oxford Dictionary, “Privacy is the state of being alone and not watched or interrupted by other people”. Cambridge Dictionary defined Privacy “as the state of being alone or right to keep one’s personal matters and relationship secret”. According to the Black’s Law Dictionary<sup>2</sup>, privacy means “the right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned”. Privacy is generally required for want of personal integrity.

The concept of privacy is as old as mankind. The ancient text of Hinduism, Christian and Muslim talks about the concept of privacy. The ancient text of Hinduism Hitopadesh says that certain matters such as worship, sex and family matters must be kept private. The Christian Holy book of Bible also incorporates the concept of privacy. It says that Adam and Eve used to cover their body with leaves so as to maintain bodily privacy.<sup>3</sup>

Privacy is very dynamic concept. Many jurists tried to define privacy but due to its swinging nature unable to restrict it to a number of words. The concept of privacy keeps on changing according to needs of the society and therefore it is not static in nature.

The modern notion of privacy was first appeared in a famous study of ‘The Right to Privacy’ published in Harvard Law Review by Louis Brandeis and Samuel Warren in 1890. In this study, the authors defined the right to privacy as “the right to be let alone”. Since then, the concept of privacy keeps on evolving and becoming a centre sphere of basic human laws.

## TIMELINE OF PRIVACY LEADING UPTO FUNDAMENTAL RIGHT IN LAW OF THE LAND

In the Indian Scenario, the concept of privacy was brought forth number of times in the debate of Constituent Assembly. The journey of Right to privacy prior to gaining independence began when The Constitution of India Bill, 1895 said that “Every citizen has in his house an inviolable asylum” and when The Commonwealth of India Bill, 1925 said that “Every person shall have the fundamental right to liberty of person and security of his dwelling and property”

Apart from this, The Nehru (Swaraj) Report, 1928 said that “No person shall be deprived of his liberty nor shall his dwelling or property be entered, sequestered or confiscate.” The first mention of privacy as an essential right was put forth by KT Shah. K T Shah’s Note on

<sup>2</sup>“Privacy”, Black’s Law Dictionary, 11<sup>th</sup> edition, 2019.

<sup>3</sup>Konvitz, M. R.: Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems, Vol 31, No. 2. p. 272 (1966).

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

Fundamental Right <sup>4</sup> said that “Every citizen of India has and is hereby guaranteed security in his person papers, property, house or effects against unreasonable search or seizure”. Further KM Munshi also stressed to bring privacy as a fundamental right in the Constitution of India. K M Munshi’s Note on Fundamental Right <sup>5</sup> said that “Every citizen... has the right to the inviolability of his home” “Every citizen... has the right to the secrecy of his correspondence” “Every person has the right to be free from interference in his family relation.

Also, Harnam Singh’s Note on Fundamental Right <sup>6</sup> said that “Every dwelling shall be inviolable” (inspired by Czech Constitution). Dr. Babasaheb Ambedkar’s Memo on Fundamental Right. <sup>7</sup> said that “The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by oath of affirmation, and particularly describing the place to be searched, and the persons or things seized. However, it was nowhere incorporated in the Indian Statute. The concept of privacy, though continuously being dealt by the courts in number of cases as a common law right.

Further, Draft approved by Fundamental Right Sub-Committee <sup>8</sup> said, “The right to the inviolability of his home – to all persons”. Final report of the Fundamental Right Sub-Committee <sup>9</sup> said, “The right to the secrecy of his correspondence – to all citizens” “The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by oath of affirmation, and particularly describing the place to be searched, and the persons or things seized.” “The right of every citizen to the secrecy of his correspondence” <sup>10</sup>

The first case which dealt with right to privacy was M.P. Sharma v. Satish Chandra<sup>11</sup>. In this case, the eight-judge bench of Supreme Court deal with the constitutionality of search and seizure with respect to infringing person’s fundamental right to privacy. The Court however denied to recognise Privacy as a Fundamental Right. Thereafter, again in the case of Kharak Singh v. State of Uttar Pradesh<sup>12</sup>, the eight-judge bench of Supreme Court denied to recognise

---

<sup>4</sup> Constituent Assembly Debate, December 1946.

<sup>5</sup> Constituent Assembly Debate, Sub- Article (1), 17<sup>th</sup> March 1947.

<sup>6</sup> Constituent Assembly Debate, March 1947.

<sup>7</sup> Constituent Assembly Debate, 24<sup>th</sup> March 1947.

<sup>8</sup> Constituent Assembly Debate, March 1947.

<sup>9</sup> Constituent Assembly Debate, April 1947.

<sup>10</sup> Venkatesh Nayak, Understanding the Right to Privacy (R2P): History, Jurisprudence and Implications for India’s RTI Regime, Presented at: The 7th Annual Convention of the Central Information Commission, available at:

<https://cic.gov.in/sites/default/files/2012/R2Privacy-Venkatesh.pdf>.

<sup>11</sup> AIR 1954 SC 300.

<sup>12</sup> AIR 1964 (1) SCR 332.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

Right to Privacy as a fundamental Right in the Constitution of India but held that the activity of night visit at someone's house amounts to violation of personal liberty.

It was only after *Gobind v. State of Madhya Pradesh*<sup>13</sup> that Right to privacy gained recognition in the Constitution of India, though not as a fundamental right but as a legal right. In this case the three-judge bench of Supreme Court held that though privacy is not expressly enshrined in the Constitution of India, still it can be traced from Right to life and personal liberty under Article 21 of the Constitution of India<sup>14</sup>.

Again, in the case of *R. Rajagopal v. State of Tamil Nadu*<sup>15</sup>, Hon'ble Supreme Court has asserted that in recent times Right to Privacy has a constitutional status. It is implicit in right to life and personal liberty guaranteed to the citizen by Article 21 of the Constitution. In the case of *People Union of Civil Liberties v. Union of India*<sup>16</sup>, The Court clearly laid down that the right to privacy is a part of the right to "life" and "personal liberty" guaranteed under Article 21 of the Constitution.

Thereafter, the landmark case recognising Right to Privacy as a specific Fundamental Right under Article 21 of the Constitution of India came into being. This landmark case is Justice (Retd.) K.S. Puttaswamy v. Union of India<sup>17</sup>, wherein it was held that Right to privacy is an intrinsic part of Right to life and personal liberty under Article 21 and as a part of freedoms guaranteed by Part III of the Constitution of India. Khehar, J., wrote: "the right to be let alone is a part of the right to enjoy life. The right to enjoy life is, in its turn, a part of the fundamental right to life of the individual."

Justice Dr. D.Y. Chandrachud held- "Privacy is concomitant of right of individual to exercise control over his or her personality. It finds an origin in the notion that there are certain rights which are natural to or inherent in human being".

### **PRIVACY AS A RIGHT IN OTHER LAWS**

Apart from the Constitution of India, Information Technology Act, 2000<sup>18</sup> as amended by the Information technology (Amendment) Act, 2008<sup>19</sup>(hereinafter referred as IT Act) read with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal

---

<sup>13</sup> AIR 1975 SC 1379.

<sup>14</sup> No person shall be deprived of his right to life and personal liberty except according to procedure established by law.

<sup>15</sup> AIR 1994 (6) SCC 632.

<sup>16</sup> AIR 1997 SC 568.

<sup>17</sup> AIR 2017 SC 1095

<sup>18</sup> Act 21 of 2000.

<sup>19</sup> Act 10 of 2009.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

Data or Information) Rules, 2011<sup>20</sup> (“the IT Rules”) also incorporates privacy laws. However, these laws are primarily formulated with respect to cybercrime and electronic privacy.

They are not concerned with the data in non-electronic form. The relevant provision under these laws which deal with privacy aspect are Section 43A of IT Act<sup>21</sup> and Section 72A of IT Act<sup>22</sup>. Section 43A of IT Act provides compensation for failure to protect data and states that “Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected”.

On the other hand, Section 72A of IT Act<sup>23</sup> provides punishment for disclosure of information in breach of lawful contract. And states that “Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both”.

Section 66E of IT Act<sup>24</sup> provides punishment for violation of privacy. It states that “Whoever,

---

<sup>20</sup> Rule 3 of 2011.

<sup>21</sup> “Compensation for failure to protect data: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected”.

<sup>22</sup> “Punishment for disclosure of information in breach of lawful contract.- Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both”.

<sup>23</sup> “Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.”

<sup>24</sup> “Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both”.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both”.

Also, Section 72 of IT Act <sup>25</sup>imposes penalty for breach of confidentiality and privacy. It provides that “Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both”.

Although there is no express legislation in India which deals with data protection, there is Personal Data Protection Bill, 2019 <sup>26</sup>which governs the processing of personal data, restrict transfer of such personal data outside India and incorporated principle of data fiduciary. This bill applies to all the governmental and private enterprises which deals with data handling.

### **DIFFERENT ASPECTS OF PRIVACY**

#### **1. Right to Privacy and Health**

In the leading case of Mr. X. v. Hospital Z,<sup>27</sup> it was held that the relationship of doctor and patient is fiduciary and thus, it is the moral and ethical duty of the doctor not to disclose confidential details of the patient with the public so as to violate patient’s right to be let alone.

#### **2. Right to Privacy and Phone tapping**

In the case of People Union for Civil Liberties v. Union of India<sup>28</sup> that right to hold a telephone conversation in the privacy of one’s home or office without interference can certainly be claimed as right to privacy. In the leading case of R.M Malkani v. State of Maharashtra,<sup>29</sup> it was held that State is bound to protect the privacy of innocent citizen.

---

<sup>25</sup>“Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both”.

<sup>26</sup> Bill No. 373 of 2019.

<sup>27</sup> AIR 1999 SC 495.

<sup>28</sup> AIR 1997 SC 568.

<sup>29</sup> (1973) 1 SCC 471.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

### 3. Right to Privacy and Narco analysis

In the case of *Selvi v. State of Karnataka*<sup>30</sup>, it was held that Narco-analysis and Polygraph test invades right to privacy of an individual if done without their consent.

### 4. Right to Privacy and Sexual identities

One of the aspect relating to right to privacy i.e., right to sexual identities was recognised in *Naz Foundation v. Union of India*<sup>31</sup> and thus right to sexual identities is embedded under Article 21 of the Constitution of India.

In a recent case of *Navtej Singh Johar v. Union of India*<sup>32</sup> The Supreme Court of India held that Section 377<sup>33</sup> of Indian Penal Code, 1860 insofar as it applied to consensual sexual conduct between adults in private is constitutional.

## ADVANTAGES AND DISADVANTAGES OF RIGHT TO PRIVACY

Let's discuss the advantages of right to privacy first:

1. **ONLINE PROTECTION:** The point itself suggests that through privacy, an individual's data is protected. Let's say, we want to give our account details to our parents, for transferring money in our account. In that case, our data is protected in such a way that the other person cannot detect it.
2. **FREEDOM OF SPEECH:** Another advantage of internet privacy is freedom of speech. We all know that we live in a country where all the citizens are given equal right to speech and expression<sup>34</sup>. Let's understand it with the help of an illustration. If we know that in our neighbourhood, someone is detected positive with COVID-19, but is not telling anyone. Even if we ask that person to kindly tell the hospital and then also, they don't tell, in that case, we may take help of internet privacy sources, such as Twitter handles, Instagram handles etc. so that our voice could be heard easily to the concerned authorities.

---

<sup>30</sup> (2010) 7 SCC 263.

<sup>31</sup> (2009) SCC Del 1462.

<sup>32</sup> (2018) 10 SCC 1.

<sup>33</sup> Unnatural offences.- "Whoever voluntarily has carnal intercourse against the order of nature with any man, woman or animal, shall be punished with 1[imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine. Explanation.-Penetration is sufficient to constitute the carnal intercourse necessary to the offence described in this section".

<sup>34</sup> Article 19 of the Constitution of India, 1949 {fundamental right; right to freedom of speech and expression}.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

3. **A GREAT HELP TO ALL THE PROFESSIONS:** Internet privacy is a great help to all the professions in sharing their knowledge to the concerned people. Let's say if there is a judge of any high court. The honourable judge wants to share his judgement only with some limited persons, he/she may upload it on his google drive and allow only some people to view or edit that judgement. Same is with other professions as well, if any doctor or any scientist wants to share his/her invention, they may take help of the internet privacy.
4. **A BALANCED SYSTEM:** With a simple trust on internet privacy, people in our country and other countries, feel free and safe to share their information on social media handles. A few days ago, I saw a video on my WhatsApp, in which there was an Ayurvedic Doctor, telling us about the air borne CORONAVIRUS, and appealing to all the people to kindly burn some of the essential things like camphor, neem leaves, mustard seeds, rock salt and others to purify our air. Hence, that doctor might be sure that the solution which he is telling is correct and will not harm anyone. Therefore, we can say that internet privacy helps an individual to trust the internet privacy sources for sharing any sort of knowledge.

#### **DISADVANTAGES**

As it is well known that every coin has 2 sides, head and tail. We have discussed the advantages, now let's discuss the disadvantages of the same:

1. **CYBERBULLYING:** We all know that in today's world, we are not in a state of trust anyone easily, due to some defaulters who treat ourself in a good way but we never know when will they take the advantage of our polite behaviour and expose us. We all know that in this era, everyone is expert in making fake-Ids to expose the innocent person. This heinous crime is termed as "CYBERBULLYING". We never know that our WhatsApp chats will be posted on our social handles with some other account. So, we must be aware of this thing.
2. **CYBERCRIME:** Cybercrime is a very heinous crime done by the criminals. If we talk from the general point of view, if we talk about a general person, a general person doesn't know how to update and keep his secret information with the other users. Hence, we should take care of our information while sharing it.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

**PRIVACY LAWS IN DIFFERENT COUNTRIES:**

Let's discuss about privacy laws in different countries:

1. **AUSTRALIA:** There is a privacy law in Australia, known as "AUSTRALIA'S PRIVACY PRINCIPLES". This law consists 13 principles in which it is prescribed everything as to how do we have to keep our personal information safe. As per the principles, each data is handled transparently. So, one must know how to keep his/her website safe and how to keep his/her personal information safe. Also, the privacy principles and the Australian law states that if any citizen of the country do not give his/her personal information, must face future consequences, which will be very worse.

2. **CANADA:** Moving on further, let's discuss about the privacy laws in CANADA. Canada's "PERSONAL INFORMATION PROTECTION AND ELECTRONIC DATA ACT (PIPEDA)", provides you the guidelines how to collect, store and use the personal data of their users or subscribers for digital marketing. Basically, this act means that the privacy policies should be accessible to the users i.e., the Canadian citizens and if they need any additional guidelines, they may refer to the Privacy toolkit in the said Act.<sup>35</sup>

3. **FRANCE:** Let's see what happens in France? France regulates its Privacy matters with the help of the "Data Protection Act"<sup>36</sup>, for collecting the data of the citizens through emails, or any other sort of information for identifying a person. This act applies to all those who are collecting data in France, that's the reason why France Data Protection Authority was able to sue Google for violating the privacy law.

4. **IRELAND:** In Ireland, there are 2 policies of privacy. One of them is the "Data Protection Act 1988 and E-Privacy Regulations 2011"<sup>37</sup> for regulating privacy in the field of electronic communication. In Ireland, there is a difference between an organization's Privacy Policy and a public Privacy Statement.

What is a privacy policy? A Privacy policy is a legal document of a company that tells us whether the company follows all the 8 privacy policies and a privacy statement is website documentation that clarifies how the data is being collected

---

<sup>35</sup>PIPEDA.

<sup>36</sup> 1978, which was latest amended in the year 2004.

<sup>37</sup>(S.I. 336 of 2011).

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

and handled on that website. Websites have a legal obligation to include privacy policy statements and they can be fined up to “100,000 Euros” for neglecting this duty.

5. NEW ZEALAND: “New Zealand's Privacy Act of 1993” states that, when collecting this type of data, you are obliged to seek any non-public personal information straight from the individual. The person whose information needs to be extracted, we have to submit our name and the purpose for requesting this data. You must also tell them whether the information is required by law, or if it is optional, and they need to be aware of their own rights regarding that data. A complaint by the user can trigger an investigation and you'll be placed under scrutiny to ascertain if you collected the data in accordance with the privacy law.

6. UNITED STATES OF AMERICA: In the US, privacy laws are not strictly regulated by federal laws as in other cases mentioned in the text. However, the US leaves it up to the state to decide on the strictness of their privacy policy.

The “FTC (Federal Trade Commission)” is invigilated to regulate business privacy laws, and they are not required to have a privacy policy, but they are prohibited from using deceptive methods.

They have also implemented a new privacy law, i.e., the “Children's Online Privacy Protection Rule (COPPA)”, which deals with those internet sources that collect information from minor children<sup>38</sup>.

The first law in the US that warrants you to post a privacy policy on your website is the “California Online Privacy Protection Act (CalOPPA)”, and it applies to any website in California that collects data from users in California.

- “CalOPPA requires that policy from websites that collect personal data to contain the following information:

- The type of personal data you are collecting
- Naming any third parties that will have access to it
- How users can review and change the collected data
- How you'll update users regarding the alterations to the privacy policy.

Your privacy policy's effective date”<sup>39</sup>

---

<sup>38</sup> Children below 13 years old [as per the USA privacy laws.

<sup>39</sup> Data collected from the USA privacy law website.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

7. SOUTH KOREA: According to the “Act on Promotion of Information and Communications Network Utilization and Data Protection in South Korea”, any personal information that is seized by the communication services provider warrants legal consent from the user.

If the consent is to be considered valid, you need to give all the necessary information such as your full name, address, account details etc.

The Framework Act on Telecommunications defines information and communication services as the following - "services that mediate a third party's communication through the telecommunications facilities and equipment or to provide the telecommunications facilities and equipment for the third party's telecommunications."

Privacy in emergency circumstances:

“The fundamental right to privacy and the general public interest”:

In order to conscientiously analyse the privacy implications of the COVID-19 pandemic, a preliminary and general discussion on privacy and personal data rights is necessary in order to ensure the temptation of partisan argumentation is resisted. As we all know that right to Privacy and the right to data protection are fundamental rights, yet they are not absolute rights. According to philosophical tradition, “a right is absolute when it outweighs every other element, including other rights and freedoms, including the moral imperative of saving human lives, and the protection of the efficiency of an economic system.”

States of emergency, national interests, and exceptional circumstances have allowed in the past for temporary limitations of fundamental rights such as the right to privacy. Having been defined as “a threat for every country, rich and poor” by the Director-General of the World Health Organisation (WHO), the COVID-19 pandemic is an exceptional circumstance which led countries worldwide to declare states of emergency. The director-general of WHO, took help of some the provisions of the UN Charter and European Union to explain the impact of right to privacy in this pandemic.

According to Art. 52(1) of the Charter of Fundamental Rights of the European Union, “limitations on the exercises of the rights and freedoms recognised by the Charter may be made

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

only if they genuinely meet objectives of general interest recognised by the Union”. Under Article 8 (2) of the said charter “In the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protections of the rights and freedoms of others.”<sup>40</sup>

Concerning health data, a legal basis for processing can be found in Art. 9(2)(i) GDPR, and further guidance is provided by Recitals 52 and 54 GDPR. According to the Regulation, the processing of special categories of personal data is permitted when it is necessary for reasons of public interest in the subject of public health, “such as protecting against serious cross-border threats to health”.

Tracking individuals to contain the spread:

- During recent outbreaks, such as “SARS”<sup>41</sup> in 2003, information and communication technology (ICT) tools were unfolded to rapidly detect sources of infection, clusters of cases and transmission routes. The COVID-19 pandemic has facilitated the dissemination of these methods and instruments, specifically with the use of location data to support the response to the pandemic and by means of tracing contacts of affected individuals to limit the spread of the virus.
- Earlier, location data was collected for the purpose of producing statistics on the aggregated movement of individuals, irrespective of their health status. Such data would allow governments to monitor the overall effectiveness of their containment measures, for instance, the prevalent lockdown being imposed in all the states. The use of location data implies that electronic communication service providers or information society service providers’ applications would share aggregated and anonymised datasets indicating the geographical position of terminal equipment (e.g., a smartphone) with public officials, allowing them to track population movements. Although using such techniques would require efforts to remove the ability of linking the data with identified or identifiable natural persons, research has shown that anonymising location data is harder than expected since mobility traces of individuals are inherently unique and highly correlated.

---

<sup>40</sup> European Union.

<sup>41</sup> Severe acute respiratory syndrome caused by the coronavirus. A severe form of pneumonia that appeared in outbreaks in 2003.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

- We all know that during this pandemic, we all are in need of oxygen cylinders, ventilators, Remdesivir injections; especially in our capital of India, in that case, it is possible only through internet privacy that the verified numbers are supplying the essentials and it is helping a lot to the common people.
- Another great initiative by our Government is that they have launched an App known as “AAROGYA SETU”, in which an individual, if facing any health issues, will directly tell the symptoms in this particular app, and if that person is diagnosed with COVID-19, then other people near that affected person will be notified through that app. Hence, we can say that internet privacy helps an individual too.

### CONCLUSION:

At the end, I just want to say that internet privacy, no doubt have some loopholes in the system, but if we take it on a positive side, internet is the only thing that gives us rapid and accurate solutions. No doubt, some defaulters are misusing it in a very bad manner, but we all know which is a trustable source? Even if we talk about a young age child, a teenager, an old person, each person relies on internet. If we talk about this pandemic, Aarogya Setu app and other medical apps help us all to rely and be aware of the affected person. Hence, we must use these apps carefully.