Page 1849 - 1853 **DOI:** *https://doij.org/10.10000/IJLMH.113242*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 3

2022

Personal Data Protection: Threats and Challenges in the wake of Covid-19

SWATI RAI [1]

ABSTRACT

For the past few 3 years the entire world has been revolving around the threats and challenges resulting from the effects of the virus named Covid-19 commonly called as 'the Corona'. The pandemic had affected the lives of the individuals in many ways posing various challenges before them. Although the mankind is very fast adapting and accommodating with the technological advancements. One such measure utilized the most for accommodating the concerns of connectivity with the outside world is the use of Internet and online applications for trade, commerce, professional activities and personal outreach. The use of Internet has indeed made easier the life of people ensuring connectivity with the outside world during the phase of lockdown and isolation world over. But at the same time the over dependence on Internet and Online resources has introduced the issues such as abuse and misuse of personal data divulged during online activities and interactions thus pawing way for various kinds of cyber-crimes. This becomes even more significant an issue considering the fact that the Indian legislative framework is inadequately armed to deal with the issues such as Personal data protection or protection of Right to privacy in the cyber world. The over involvement of Internet and virtual space and the inefficient laws are the setbacks to the proper utilization of the such significant technological boons namely cyber space.

Keywords: *Covid-19, Cyber Space, Internet, Cyber Security, Cyber Crime, Aarogya Setu App, Right to Privacy, Cyber Laws, Data Protection.*

The recent outbreak of Covid 19 pandemic has affected considerably the entirety of mankind including the physical, mental, psychological, social, religious, financial and cultural domains. The virus is in a certain way has exerted a universal control on the world affairs and therefore it will not be wrong to call the present era as the Era of Corona. It would still be early to call it post corona era in the light of the expected fourth wave of the deadly virus. In the first two years of the virus spread, to contain the virus and fight against it, the most viable option perceived had been lockdowns and social distancing. People around the globe were pulled away from the outside world and were restrained to stay within the safety of their own home. As the real-world avenues were forced to take down their shutters in the wake of Covid-19, the

[1] Author is an Assistant Professor at Department of Law, PIMR, Indore, India.

 [ISSN 2581-5369]

people were forced to be largely depending on the cyber space for sustaining their day-to-day activities. As the individuals were temporarily forced into isolation to achieve social distancing, the internet was their only window into the world. Entire swaths of society including the young and the old, the employed and the unemployed, the professionals and the students, the organized sectors and the unorganized sectors, the public entities and private entities, had all taken refuge in the cyber world not only for their professional and economic activities but also for finding peace and solace had moved online from within the safety of their home. Although the world has adapted itself to live and sustain amidst the Covid virus and have now moved to the physical world withdrawing all the lockdown norms and resuming the normal day to day activities, but still a large section of the society and economic world has retained the virtual space of operating as their normal mode since. Many sectors such as IT is still working in online mode from virtual workplaces. Thus, we can see that the present times have seen the involvement of people in virtual space and presence in the cyber space and dependency on internet much more than ever.

While the online world is often portrayed as a societal ill and a potent threat, this pandemic is a reminder of how much the cyber world has to offer at all fronts. The Internet not only foster a sense of connectedness amid social distancing but is evolving as the most potent alternative avenue for all the professional and economic activities from well within the comfort and safety of a person's own abode. Even the education sector that was largely depended on the personal interaction and real time spaces has shifted very conveniently and efficiently to the digital platform via online communication platforms. Not just the individuals but also the Government of India is utilizing the digital platform in adapting itself to fulfill the changing needs of the society.

Though it cannot be denied that as the dependence of the society has been increasing so rapidly and vividly on the internet and the cyber space in the wake of this pandemic and the aftermath, it also lays bare the many vulnerabilities so created by this overwhelming dependence on the internet and cyber space. The segments of the population that were once away from the reach of cyber vulnerabilities are now well within its target range. To mention a few, these threats include the dangerous consequences of censorship, the constantly morphing spread of disinformation, supply chain vulnerabilities and the risks of weak cybersecurity. Like any other potent opportunity of launching malware attacks, the Covid-19 pandemic has sparked an increase in phishing and ransomware attacks[2]. There has been a considerable surge in phishing attacks using pandemic-related misinformation in the hopes of gaining access to credentials

[2] www.govtech.com

 [ISSN 2581-5369]

and other personal information or to deploy malware[3]. One of the most common and convincing trends is to feed on the fear generated by the uncertainties amidst the Corona era thus using the health guidance, containment and infection rate news, medication and cure against corona, testing and assessing applications and also employment and financial security providing platforms as the phishing threats.

To deal with these increased threats of cyber security and cyber-crimes, a lot of preventive measures have been advised by the cyber experts. At the general level the experts advice to educate people and create awareness among the masses of the common characteristics of the treats exploiting the Covid 19 related concerns and be vigilant in not falling prey to the scams like fake charity donations, updating insurance and banking related credentials, installation of applications that provides updates on corona, etc., thus spilling away the personal details in most of the cases. Experts say existing security defenses, such as email scanning, VPNs and multifactor authentication, may need to change more to adapt to an increase in remote workers and new phishing lures[4]. And, more importantly, users need to be more vigilant and understand how attackers prey on them.

At the organizational level the suggested preventive measures include auditing networks for weaknesses, implementing or expanding the use of VPNs, updating software, and educating employees about phishing techniques, organizations filter emails with coronavirus-themed content, unusual attachments, pandemic-related domains on commonly abused hosts, name servers and unusual top-level domains. With awareness and caution the threats posed by the increased cyber-criminal activities can be prevented and mitigated to a certain level. But when talking about the larger picture with the stricter legal norms and regulations to deal with the cyber security threats the focus shifts to the legal fraternity.

At this juncture, the most potent question posed to the law fraternity is related to the efficiency and efficacy of the existing legal framework in dealing with the varied and vivid crimes emerging as a side effect of the pandemic of Corona worldwide. The entire legal framework is under review and is adapting itself according the changing nature of the living activities and the issues related thereof. Among the various laws, the cyber laws take the center stage of discussion owing to the considerably major shift of the masses from the real world to the virtual space thus opening up avenues of varied forms of criminal activities to be dealt with.

---

[3] https://www.techtarget.com/searchsecurity/feature/Coronavirus-phishing-threats-force-heightened-user-awareness

[4] https://www.techtarget.com/searchsecurity/feature/Coronavirus-phishing-threats-force-heightened-user-awareness

 [ISSN 2581-5369]

Speaking of our own country India, the cyber laws have been under consideration and are due amendments in the wake of evolution of law of privacy and other incidental issues. With the current development of affairs, there arises a need for further deliberations on the existing cyber laws and the need for it to adapt to the changing scenario. Currently we have the Information Technology Act, 2000 and its corresponding rules under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 as the only existing framework of laws to deal with cyber-crimes in the nation. As far as the Data privacy and protection of personal data is concerned, the Privacy Bills were drafted in 2011 and 2014 and Personal Data Protection Bills were drafted in 2013, 2018 and 2019, but no legislation has been made for protection of privacy and personal data till day. The Personal Data Protection Bill that is pending the approvals cannot be considered as a comprehensive piece of legislation adequate for protecting and preserving the personal data of the individuals from abuse and misuse by the various authorities and organizations with whom the data has been shared. The said bill does not contain provisions for protecting personal data shared voluntarily or data divulged to the government agencies, thus leaving the individuals vulnerable and without remedy in case of any misuse or abuse of their personal data.[5]

One such case study is that of the compulsory installation and use of Aarogya Setu application mandated by the Government of India as a tool to keep an active vigil on the spread of the pandemic of Covid-19. During the pandemic spread, the Government of India adapted and used digital platform for fighting against the pandemic and preventing its spread. Of the many initiatives of the government, one such significant step was the application named Aarogya Setu. Aarogya Setu the mobile application is developed by the Government of India to connect essential health services with the people of India in the combined fight against COVID-19[6]. This app was used as a tool for creating awareness, managing the data of the affected people, monitoring the spread of the virus among the masses and connecting government and the people. The App aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19. Not only this but also the other services like supply of essential commodities, registrations and reservations for the travel, issuance of E-passes by the authorities, information on the

[5] The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.
The Bill includes exemptions for processing data without an individual's consent for "reasonable purposes", including security of the state, detection of any unlawful activity or fraud, whistleblowing, medical emergencies, credit scoring, operation of search engines and processing of publicly available data.

[6] https://www.aarogyasetu.gov.in/

medical assistance etc, was all done very efficiently and effectively through digital platform. The use of the application requires for the disclosure of the personal credentials along with the continuous access to the GPS location of the user. The application has been so far perceived as an active tool in the hands of the authorities to monitor the movement of the people affected and non-affected by the virus though at the expense of the violation of privacy of the individuals. The question that ponders is pertaining to the legal aspects of the use and the misuse of this mobile application of Aarogya Setu as it deals with a substantial data of the individuals that might be exploited for a number of economic crimes and cyber-crimes.

The Honorable Supreme Court of India has declared Right to privacy as a fundamental Right under Article 21 of the Constitution of India in the much-celebrated case of Justice K.S. Puttaswamy (Retd.) v. Union of India[7]. This Fundamental Right of privacy is guaranteed against the State and therefore the Personal Data of individuals in the possession of the Government and government authorized agencies also seeks proper safeguarding and security from any unauthorized use or abuse of the same. The existing legal framework is inefficient and inadequate to cater to the concern of personal data protection and that has been a major concern lately for the government, legislators, agencies and individuals. The need for hour is that the Indian legislative framework on privacy protection has to be updated and upgraded as per the international norms addressing the issues and concerns of data protection and cyber security and at the same time balancing the same with the much-needed digitalization of the information and day to day activities for the socio-economic growth in the country. In this context, the Government of India is entrusted with the responsibility of framing laws and policies on data protection ensuring at the same time the Right to privacy and digital transformation for the socio-economic growth of the country.

*****

[7] (2017) 10 SCC 1

 [ISSN 2581-5369]