International Journal of Recent Advances in Multidisciplinary Topics
Volume 3, Issue 1, January 2022
https://www.ijramt.com | ISSN (Online): 2582-7839

Does the Use of Intrusive Artificial Intelligence during the COVID-19 Pandemic Violate Human Rights

Sarvadh Sathiaram*
Student, Akshar Arbol International School, Chennai, India

***Abstract*: The COVID-19 pandemic saw the introduction of various AI apps for contact tracing and also for tracking the movement of people within cities and between cities, and countries. While these apps were very useful to curtail the spread of the virus, they also in many ways threatened to violate some of the core values of human rights in many countries.**

***Keywords*: Apps, Artificial Intelligence, COVID-19 pandemic, Human Rights, Right to be Forgotten, Right to Privacy**

1. Introduction

This article explores the human rights impacts of the use of artificial intelligence technologies, especially during the COVID-19 pandemic. During the COVID-19 pandemic, many governments have used various artificial intelligence (AI) apps to track the crisis. While these technologies help provide useful information, they also threaten to violate some of the core values of democracy and human rights. This article explores whether this use of AI violates human rights in the context of maintaining the collective health of the community. This may not be a new question. Nevertheless, it is still a pertinent one especially in today's context as these technologies are becoming an integral part of our everyday lives. I am particularly interested in studying this conundrum of how society can enjoy the benefits of AI without compromising our fundamental human rights and our individualities.

2. What is Artificial Intelligence (AI)

A founding father of AI, John McCarthy, defined AI as, "The science and engineering of making intelligent machines, especially intelligent computer programs, related to the similar task of using computers to understand human intelligence. It is the study and use of machines that can think and act like or even in some instances do better than humans." 1 (McCarthy, What Is Artificial Intelligence?).

1) Intrusive AI

While AI is particularly useful in simplifying several tasks, it can also be an intrusive technology. Some examples of intrusive. AI include mass surveillance systems, profiling software, facial recognition technology, and personal data collection software. To determine the level to which intrusive AI infringes on our privacy and rights, we must first understand human rights and their importance to society.

2) What are Human Rights?

According to the United Nations, "Human rights are defined as rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status." Human Rights are universal and binding. "International human rights law lays down the obligations of Governments to act in certain ways or to refrain from certain acts, in order to promote and protect human rights and fundamental freedoms of individuals or groups."2 (United Nations, Human Rights). It is critical to protect the human rights of every individual because they reflect the minimum standards for people to live with dignity.

3. Identifying the Human Rights Consequences of AI during the COVID-19 Pandemic

In the current COVID-19 pandemic, due to the use of various technologies, there is the potential for human right violations such as people's right to move freely; their right to privacy and data protection, and their right to be forgotten (the right to get one's personal data deleted without undue delay.3 (General Data Protection Regulation EU, Everything you need to know about the "Right to be forgotten"). The widespread effects of the pandemic have prompted many governments to develop and use various technologies to track the spread of the virus, collect people's personal and medical information, and track their movement and those individuals with whom they have come into contact.

While governments may need some of this information to control the virus's spread, this also poses a critical ethics question:

"Are these tracking apps and technologies intruding our fundamental human rights, and if so, to what extent is this intrusion acceptable?"

Many countries have built technologies and apps for contact tracing, tracking the virus spread, identifying locations of infected people, and even quarantine apps. These apps have

*Corresponding author: sarvadh.s@gmail.com

shown early benefits by helping governments to contain the spread of the virus, limit exposures by isolating containment zones and even notify people where to go and where not to go.

While these technologies have been developed keeping COVID-19 tracking in mind, there are several questions that arise about the legitimacy of these apps such as the data they collect and with whom they might share that information. This presents several human rights consequences that make us wonder if all these apps and its benefits come at an inevitable cost to our privacy.

4. Global Perspective

There are over twenty-five COVID-19 apps that are being used by governments. Some of the early apps developed include Italy's Immuni, Singapore's TraceTogether, Israel's HaMagen and UK's NHS COVID-19 app.4 (O'Neill, A flood of coronavirus apps are tracking us. Now it's time to keep track of them). These apps work by collecting health data and tracking its users based on location to alert authorities in case of any contact with infected persons. Many of these apps are still voluntary in nature but some of them like Bahrain's BeAware, China's Health Code system, Qatar's Ehteraz, and India's Aarogya Setu are being mandated, directly or indirectly, for all its citizens.

These apps require citizens to provide access to their personal devices, personal data, medical history, biometric data, and travel and movement data. In some cases, such as China's Health Code System, they even track purchase and payment information. Iran's Mask.ir app has been alleged to be more of a spying app by many experts prompting Google to remove the app from its Play Store.

In addition, some apps even curb the movement of its citizens based on the information they enter, thereby fundamentally violating people's right to freedom of movement. For example, the Chinese Health Code system accords "color code" to its users: green means they can go anywhere, yellow denotes a 7-day quarantine and red mandates a 14-day quarantine. 5(Wang, China: Fighting COVID-19 with Automated Tyranny). Many residential complexes have this Chinese app linked to their access control system thereby denying access to people who have yellow or red codes. Another development in Hangzhou China has been the development of a "points- based system" where citizens will receive a daily score based on their activities – positive points for healthy activities like walking 15,000 steps a day, or for 7½ hours of sleep and negative points for unhealthy practices such as consuming 200ml of Chinese alcohol per day or smoking 5 cigarettes a day.

5. National Perspective

India launched its own COVID-19 app called "Aarogya Setu" or "Bridge to Health" in April 2020. The app works using GPS and Bluetooth and tries to determine a person's risk based on his/her location and who he/she has come in contact with. It is the largest downloaded COVID-19 app in the world and by May 15, 2020, there were more than 100 million users of this app in India. The Aarogya Setu app is not fully "open source" thereby making it a bit difficult for independent analysts and researchers to audit and ascertain the app's capabilities.

The Aarogya Setu app has done exceptionally well in terms of contact tracing and controlling the spread of the COVID-19 virus throughout the pandemic. In addition to this the COVIN app which is another invaluable app that has been recently developed by the Government, has been very useful in terms of locating vaccinated and non-vaccinated persons and helping local Corporation bodies in planning vaccination drives and efforts to ensure the majority of the country is vaccinated before end of December 2021.

While the apps are very useful one needs to be cautious to ensure that all the data collected in these platforms are kept confidential and don't get into the hands of malicious entities and the Government has to take adequate precautions to ensure data privacy and protection.

6. Personal Perspective

Data is like a knife. It can be used as a surgical tool to save someone's life or as a weapon to take someone's life. It depends on the user, how they use it, and their intentions. I agree that the COVID-19 apps can be quite useful in containing the virus and ensuring public health and safety. However, I believe that the violation of fundamental human rights pertaining to privacy and data protection can lead to precarious situations and outcomes.

Firstly, mandating these apps, whether directly such as in Bahrain or Qatar gives rise to several legal and ethical questions. Secondly, many of these apps intrude on one's right to freedom of movement. The "color code" given by Chinese health App determines one's ability to move around and earn a living. In addition, Hangzhou's callous health points system is a blatant infringement on one's privacy under the pretext of societal benefit.

7. Possible Scenarios

While all of these apps may help in tracking and containing the virus, and can aid in research and vaccine development, only time will tell us what the real benefits are. One possible scenario is when the government withdraws these apps and deletes the data post the pandemic so that people can once again return to their normal lives. Another plausible scenario is that the data continues to be obtained and stored, making it accessible to governments and other external agencies post the pandemic. This raises a key question about the fundamental "right to be forgotten". Personal data must be erased immediately when the data is no longer needed for their original purpose. But, after this pandemic ends, would all the data be deleted? If so, by whom and by when? Who is responsible for this action?

There is also the danger of hackers misusing this data. Recent case studies only further substantiate this concern. For example, the incident of the True caller app data which was sold on the "dark web" thereby comprising personal information of 40 million Indians only raises more concerns on the potential misuse of the COVID-19 data. And of course, one cannot ignore the direct sale of the data by governments.

8. Possible Courses of Action

Whether the governments themselves have any malicious intent or not, the fact remains that all this captured data is vulnerable for misuse if fallen into the wrong hands. There is no guarantee that it will not be used for vicious purposes such as blackmail, extortion, or worse. Moreover, governments can also use this data to further their own agenda, such as manipulating elections through targeted voting campaigns, discouraging candidates who oppose them with data leaks, etc. Therefore, unless there is a mature and evolved society with enough built-in checks and balances, these potential risks far outweigh the benefits. Governments must design necessary controls and craft public policy with the goal of preserving human rights while retaining the benefits of AI.

9. Personal Response

Human rights are essential to human dignity. Compromising individual rights during a pandemic or at any other time could lead to exploitation by governments and private entities. We as users are equally responsible for what data we put out there by taking the necessary precautions to avoid unwanted exposure. I performed an audit of my phone and iPad and uninstalled all the unwanted apps. I also became more aware of the information I put on various social media sites. I educated myself and my family members about the potential risks. I also helped my grandfather uninstall unnecessary apps on his phone and denied access to his contact list to several of the apps. I will continue to talk and write about these potential risks so that we can all become more proactive when it comes to protecting our personal information.

10. Conclusion

Over the last century, with various scientific and technological discoveries, human beings have faced different types of ethical challenges. It is important to understand that these technological changes are supposed to enhance our quality of life, not to limit or restrict our individual rights and freedoms. With AI, we find ourselves once again, at a crossroads. It is up to us as responsible citizens to create systems, policies, checks and balances that ensure that no technology will deny our human rights.

After all, as Nelson Mandela so famously stated, “To deny people their human rights is to challenge their very humanity.”

References

[1] “Coronavirus Must Not Be Used as an Excuse to Entrench Surveillance.” ARTICLE 19, 9 Apr. 2020,

[2] Zhong, Raymond. “China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears.” Baltimoresun.com, 28 May 2020,

[3] “Covid-19 Apps Pose Serious Human Rights Risks.” Human Rights Watch, 13 Apr. 2020

[4] Doffman, Zak. “Coronavirus Spy Apps: Israel Joins Iran and China Tracking Citizens' Smartphones To Fight COVID-19.” Forbes, Forbes Magazine, 15 Mar. 2020,

[5] Russell Brandom, Adi Robertson. “Apple and Google Are Building a Coronavirus Tracking System into IOS and Android.” The Verge, the Verge, 10 Apr. 2020.

[6] Weber, Jonathan, and Paresh Dave. “The Race to Deploy COVID-19 Contact Tracing Apps.” Edited by William Maclean, Reuters, Thomson Reuters, 14 May 2020,

[7] Doffman, Zak. “COVID-19's New Reality-These Smartphone Apps Track Infected People Nearby.” Forbes, Forbes Magazine, 8 Apr. 2020,

[8] Mozur, Paul, et al. “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags.” The New York Times, the New York Times, 2 Mar. 2020.

[9] Greenberg, Andy. “India's Covid-19 Contact Tracing App Could Leak Patient Locations.” Wired, Conde Nast, 6 May 2020.

[10] Cimpanu, Catalin. “Spying Concerns Raised over Iran's Official COVID-19 Detection App.” ZDNet, ZDNet, 9 Mar. 2020.

[11] Co-Pierre, George. “'Track and Trace' Is Key to Containing COVID-19: How Privacy Can Be Protected.” The Conversation, 27 May 2020,

[12] Chaturvedi, Aditya. “The China Way: Use of Technology to Combat Covid-19.” Geospatial World, 11 May 2020.

[13] Andrew Crocker, Kurt Opsahl. “The Challenge of Proximity Apps For COVID-19 Contact Tracing.” Electronic Frontier Foundation, 29 Apr. 2020.

[14] Hart, et al. “Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 While Mitigating Privacy Risks.” Harvard University - Edmond J. Safra Center for Ethics, Edmond J. Safra Center for Ethics, 2020, pp. 1–38.

[15] Wong Professor of Political Science, Wendy H. “Technology Threatens Human Rights in the Coronavirus Fight.” The Conversation, 23 June 2020.

[16] McCarthy, John. “WHAT IS ARTIFICIAL INTELLIGENCE?” Computer Science Department, Stanford University, 2007.

[17] O'Neill, Patrick Howell. “A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them.” MIT Technology Review, MIT Technology Review, 23 June 2020.

[18] Wang, Maya. “China: Fighting COVID-19 with Automated Tyranny.” Human Rights Watch, 1 Apr. 2020.