Chapter 4

Data collection, privacy, and security: evolution of the right to privacy in times of COVID-19 crisis

Dao Thi Nguyet

Abstract: The development of Digital and Information Technology has changed our lives forever and its impact on our privacy. In the Digital Age of the 21st century, we have witnessed the government's effort to protect citizens' data from global corporations until more recently with the outbreak of the Covid-19 pandemic. This paper analyzes how the right to privacy has evolved and more specifically in times of crisis, namely the COVID-19 pandemic.

Keywords: Covid-19, privacy right, data security, data privacy, data collection, personal information

Introduction

Privacy was born with the advent of the state. Privacy rights have since then been created and transformed, evolving alongside of human society's development and individualism. Privacy rights have increasingly become one of the most critical human rights issues of the modern age. It has been recognized in international conventions and treaties. The interest in privacy increased rapidly in the 1960s and 1970s with the advent of information technology. And in recent years, computer systems' capabilities in monitoring and archiving have substantially impacted personal privacy.

Therefore, the need to promulgate specific regulations governing the collection and processing of personal information emerged. While the debate over privacy and the state's role in protecting this right are far from over, the outbreak of the Covid 19 pandemic has stirred the privacy debate in a different direction and brought it to a new level of discussion. How much privacy a person would compromise and how much control over personal data the state can take to protect a person's health and community's safety when they approach epidemic prevention depends on personal information. The Covid-19 crisis is an unexpected circumstance for us to witness the evolution of the right to privacy. And unfortunately, we see a milestone in the irreversible decline of privacy rights.

Privacy and the right to privacy

The concept of privacy was first discussed in the essay "The Right to Privacy," with recognition of "the right to let alone," or in other words, the right to control information about oneself[86]. This conceptualization of privacy still holds true today, understood as an individual or group's ability to seclude themselves or information about themselves and express themselves selectively.

In 2004, the Electronic Privacy Information Center and Privacy International Organization published a report "Privacy and human rights: an International Survey of Privacy Laws and Practice[87]." They report studies the content of the law on privacy protection in 50 countries since 1997, noting the following fundamental facets: Information Privacy (involves rules governing the collection and handling of personal data), Bodily Privacy (concerns the protection of oneself against invasive procedures such as drug tests), the privacy of communications (covers the security and confidentiality of mails, telephones, all kind of communication forms) and Territorial privacy (concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space).

---

[86] Warren, S. and Brandeis, L., (1890), "The Right to Privacy," *Harvard Law Review*, 4: 193–220.

[87] David Banisar, Simon Davies; Privacy and Human Rights: An international servey of Privacy Laws and Developments, The John Marshall Hournal of computer & information law, 1999.

Why should we care about privacy? Privacy is a matter of dignity and autonomy. This right helps each individual create and control legitimate boundaries with others, thereby protecting him or herself from arbitrary interventions in life and allowing each individual to define who he or she is and how he or she wants to interact with the world around them. On behalf of social benefits, protecting each member's right to privacy also creates and protects the foundation of community life. Communities cannot survive if their members are not protected from all forms of abuse. Briefly, privacy establishes a line between public and private spaces. More importantly, this right supports and reinforces other rights, including freedom of expression and association freedom.

Once humans recognized the importance of privacy, legal terms and definitions were built to protect it. Privacy rights are most simply the right of a person to be let alone, be free from unwarranted publicity, and to live without unjustified interference by the public in matters with which the public is not necessarily concerned[88]. Privacy rights are mentioned in more detail in article 12 of the Universal Declaration of Human Rights, 1948 (UDHR)[89]: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks". The right to privacy is reaffirmed in Article 17 of the International Covenant on Civil and Political Rights, 1976[90]*:* "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks". It is also mentioned in the constitution of 150 countries around the world.

---

[88] *Strutner v. Dispatch Printing Co.,* 2 Ohio App. 3d 377 (Ohio Ct. App., Franklin County 1982).

[89] Universal Declaration of Human Rights, 1948, https://www.un.org/en/universal-declaration-human-rights/.

[90] International Covenant on Civil and Political Rights (1967), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

Data privacy and data security

People are often confused between privacy and data privacy that are related but not the same. While privacy describes the state of keeping oneself from another, data privacy is concerned with the proper handling of personal information, including collecting, processing, storage, sharing, consent, and regular obligations[91]. Data security concerns include policies, methods, and means to secure personal data or information data[92]. There are three pillars of data security: "*Confidentiality* – prevents sensitive information from reaching wrong people while making sure that the right people can use it; *Integrity* – maintains the consistency, accuracy, and trustworthiness of information over its lifecycle; and *Availability* – ensures that the information is available when it is needed[93]."

Recently, personal data has become a new precious commodity that commercial and political entities significantly desire. Despite paperwork provisions asserting that individual information is vital, everyone must respect it, and that states must ensure its protection, the privacy right is theoretical, while data protection is practical. Entities, like states or companies, can arbitrarily collect and use personal data, they can easily access individual thoughts and observe individual activities. If this threat materializes one day, personal freedom and personal privacy will no longer exist. New forms of protection are therefore urgently required.

Privacy data protection remedy

Privacy is a value that underpins human dignity and other fundamental rights. Therefore, free and democratic societies require respect for individuals' autonomy and limits on both state and private organizations' power

---

[91] Data Privacy Manager (2021), Date privacy and Data security: Definition and Comparison, https://dataprivacymanager.net/security-vs-privacy/.

[92] Ibid.

[93] Ibid.

to intrude on that autonomy. However, technological and administrative changes progressively undermine even those privacy protection regulations that existed. We have seen the law fail to keep pace with technology's rapid development at the beginning of the 21st century. Nonetheless, the good news is that the importance of data and awareness about data protection has increased. We see 128 out of 194 governments promptly proposing and adopting new laws protecting personal data. Africa and Asia show a similar adoption level, with 55% of countries adopting such legislation, from which 23 are least developed countries[94]. Europe is at the forefront of privacy protection with the enactment of the General Data Protection Regulation (GRPR) in 2018, which establishes seven principles to follow when processing data:

> 1) Legality, fairness, and transparency: The handling of data must be legal, fair, and transparent to the data subject; 2) Limit the purpose: The purpose of data processing must be legal and clearly shown to the data subject when collecting; 3) Minimize data: Collect and process data only when it is absolutely necessary for the intended purposes; 4) Accuracy: Personal data must be kept accurate and up to date; 5) Storage Limits: Store personally identifiable data only for as long as necessary for the intended purpose; 6) Integrity and Confidentiality: The processing of data should be performed on a basis ensuring appropriate confidentiality, integrity, and confidentiality; 7) Accountability: It is the data controller's responsibility to demonstrate compliance with the GDPR with all of these principles[95].

On the contrary, China's government not only fails to protect citizens' privacy, but actively invades it. China currently collects a larger than ever amount of data on its citizens, with 20 million surveillance cameras amassing a vast amount of biometric information daily. The Chinese government

---

[94] UNCTAD, Data protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[95] General Data Protection Regulation EU (2018), https://gdpr-info.eu/.

also does not issue enough laws to protect personal data from private extortion and fraud [96] [97].

Data Privacy is recognized in international covenants but getting treated differently worldwide. Even in some extraordinary circumstances, when everyone's safety in society is in danger, the right to privacy is not absolute. It means the right can be temporarily interrupted. Nonetheless, countries should only collect private information if it is essential to ensure society's common good. Legal interventions in personal life must be regulated in law and in accordance with other ICCPR regulations. General comment No.16 adopted at the 31st session of the 1988 United Nations Human Rights Commission clarified some aspects of this right[98].

We have been witnessed many cases when a state has restricted the right to privacy by justifying its activities, ranging from from terrorism prevention to state security. Currently, in the face of the unexpected danger of Covid-19, we have seen measures taken by countries designed to limit the virus's spread, while at the same time intruding privacy, both authoritarian and democratic ones.

How data has been collected and processed during the COVID-19 pandemic

There are millions of confirmed cases of COVID-19 across the world. A pandemic of this magnitude and intensity has never been experienced on a global scale like this before. In response, many policies have been developed for its detection, treatment, and prevention. After coming across the

---

[96] Emily Feng (2020), In China, A new call to protect data privaccy, https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy?t=1618142211789, NPR news.

[97] Privacy International, and the Law and Teachnology Centre of the University of Hong Kong (2013), The Right to Privacy in China, Stake Holder Report UPR 17th Session-China.

[98] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

Covid infection mechanism, various approaches have been made including, awareness hygiene improvement, social distancing practices, quarantine, isolation, and contact tracing. (Zeeshan Abedin, 2020).

However, when it comes to finding a balanced approach between helping to track and trace people in order to contain the virus and at the same time safeguarding individuals' privacy it has proven difficult to determine where to draw the line. On the one hand, digital solutions help save lives by spreading health messages, increasing access to remote physical checkups and health alerts. Simultaneously, surveillance tools that trace individuals' location and contacts present profound privacy challenges, data protection rights, and freedom of information. In many countries, we witness that privacy standards have been unlawful even though many concerns about personal privacy have been raised.

Contact tracing is a process of identifying people who have recently contacted an infected Covid -19 individual. This method aims to prevent people from getting the virus by not contacting someone who has the virus. However, there are asymptomatic carriers who are infected with the virus but show no signs. Therefore, at the beginning of the pandemic, when there were no vaccines yet, the governments used social distancing and technology to track past positive patient contacts to stamp out an outbreak. However, interviewing people infected to get information about the people they have been exposed to for two weeks is impossible because of subjective and objective factors such as not fully remembering who they were with, or not giving accurate information. That is why many countries have come up with solutions to use smartphones and apps for contact tracing. This mobile tracing works by aggregating the data inside the device to monitor the owner's mobility and tracking the mobile phones of those suffering from COVUD-19 to find out suspected patients. The government, mobile network operators, and technology companies/financial services providers collaborated in the mobile tracing strategy.

Governments around the world are adopting various strategies to track and isolate COVID-19 patients. China has developed a smartphone app named "Health code" that allows contact tracing and notification of an

infected person. In the United States, the first contact tracing call center was announced by the state of Massachusetts. This call center was planned to be managed by 1000 virtual assistants. The US federal government announced a $500 million package for the CDC to address COVID-19 surveillance. To track the level of exposure to COVID-19, the South Korean government built a map of cell phone data that was kept public. Telecommunications and credit card companies also provided data. In Israel, the government uses GMS call detail records to track patients' mobile phone data and to locate their position, contacts, and movement patterns. Few countries like Italy, Germany, and Australia collaborated with telecommunications providers and shared their location and data with the health authorities. Singapore uses a Bluetooth-based mesh network through a mobile application to detect people's proximity to those suffering from COVID-19. It gives them the warning to get tested if they come into close contact after detecting such people. Iranians collaborating with government endorsement campaigns for COVID-19 developed a mobile application where people were allowed to self-diagnose themselves and the application also discretely collects user's location data (Iniobong Ekong, 2020). India quickly joined a host of other countries that have used mobile applications to collect and disseminate COVID-related information by introducing the controversial 'Aarogya Setu' App to enable contact tracing, improve situational awareness, and publish relevant information to the public. The App's download and use were made mandatory for all public and private sector employees by the Ministry of Home Affairs in its notification on April 29, 2020 [99]. Vietnam, a successful case in preventing Covid-19, also has its own App for tracing people's social contacts. The app names Blue Zone using Bluetooth Low Enverzy's waves to log when two phones are within two meters of each other[100].

Health reporting, including COVID-19 testing, temperature testing, public- and private-sector health surveys, public authority, and internal corporate

---

[99] Financial Express (2020), Why data privacy must be safeguarded, even in times of COVID-19, *https://www.financialexpress.com/money/why-data-privacy-must-be-safeguarded-even-in-times-of-covid-19/1963579/.*

[100] Luu Quy (2020), Contact tracing app most download free app, Vnexpress News, https://e.vnexpress.net/news/life/trend/contact-tracing-app-most-downloaded-free-app-4201014.html.

reporting, collects massive personal data. The National Health Service (NHS) in the UK has submitted a document marking a change in patient data policy, giving staff more freedom to share corona-related information. Specifically, it refers to using data to understand viral trends, effects and manage patients with/or at risk of Covid-19, including positioning, exposure, screening, and tracking those patients. There is an evident trend that governments are increasingly using the collection, processing, and sharing of personal health and behavioral data on a larger scale, including the targeted monitoring of individuals to prevent the spread of COVID-19.

Data privacy and security has changed in times of the COVID-19 crisis

The importance of protecting personal data has grown steadily since the digital evolution as data collection, storage, transfer, and analysis have become simpler. Technical developments such as the Internet, Email, mobile phones, video surveillance, and electronic payment methods create new data collection possibilities. Both public agencies and private businesses are interested in personally relevant information. National security agencies want to improve their fight against crime through such means as racial profiling and telecommunications surveillance, and banking transactions from financial institutions to discover tax violations. Businesses hope to increase productivity by supervising employees and hope customer profiling will help with marketing. In their eyes, the protection of personal data has little or no practical importance. When analyzing the relationship between stakeholders and personal data, we see that entrepreneurs maintain their perspective of prioritizing their profits in whatsoever situation. However, there is an evolution in government and ordinary people's views.

Citizens' perspective

When it comes to individual privacy and data collection by businesses to follow consumer preferences, many people either may not care (thinking they have nothing to hide) or may not be informed about what is actually entailed. Consequently, it has been relatively easy for authorities to

collect data on people when the COVID -19 pandemic hit, especially when the authorities justified their actions for the sake of people's protection. However, some individuals have voiced concerns about their privacy being breached and are pessimistic that the government will continue to violate individuals' privacy from this precedent.

Government's perspective

In the 21st century, in the face of the rapid development of technology, many governments have seen the danger of privacy infringement coming from technology companies. In response, governments have enacted new regulations along with changes in technology to protect people's data. However, when the pandemic hit, many governments have foregone privacy concerns for human security. They have advocated implementing digital technologies to collect, analyze, process, and share data to deliver effective solutions for the pandemic. Few countries have legal frameworks in place to support these preventing Covid-19 measures; for instance, the Republic of Korea with Infectious Disease Control and Prevention Act allows for the collection of personal data if "necessary to prevent infectious diseases and block the spread of infection[101]," Israel permits the use of technology for tracking infected persons by monitoring mobile phones for emergency measures. However, many countries have passed new laws specifying how data will be collected and processed. Italy for example published a Degree in 2020 for collecting and sharing personal data health by public health authorities and private companies during an emergency[102]. Germany proposed the Infection Protection Law allowing the Federal Ministry of Health to require risk individuals to identify themselves. Nevertheless, many experts and citizens have spoken out to some of the methods that have been controversial over the risk of violating the privacy and other fundamental rights of citizens, especially when those measures lack transparency and publicity.

---

[101] Infectious Disease Control and Prevention Act, Article 76–2.

[102] Veronica Pinotti, Patrizia Pedretti & Martino Sforza; COVID-19 and Data Protection Compliance in Italy; Whitecase, 2020, https://www.whitecase.com/publications/alert/covid-19-and-data-protection-compliance-italy.

Trade-offs between the right of privacy for health security

Data can be used for manipulation and control. Any form of follow-up of a person infected with the virus risks inducing surveillance and privacy violation that destroys personal freedom. Before the Covid -19 pandemic, when faced with the risk of data collection and loss of privacy, most people quickly compromised privacy for comfort and accessible products and services. But when faced with the danger of the epidemic, the trade-off has changed. The justification now is between privacy and safety, without the consideration of human rights or freedom.

The relationships of data use has also changed. Public sectors are heavily involved in collecting and using data instead of private ones. Instead of playing as the protector and implementing regulations to protect citizens, governments use common safety to justify and use laws to legalize their activities. The change also leads to different consequences. Private sectors use data to control and manipulate customers' behavior to seek maximum profit; therefore, results lie in the economic field. Public sectors use data to control and influence political and social behavior, which is much more dangerous because of the threat of losing civil rights and challenging democratic governance.

On the risk of privacy rights being violated on a large scale, the World Health Organization published a joint statement on Data Protection and Privacy in the COVID-19 Response[103]. The European Data Protection Board[104] and the Council of Europe[105] have released similar statements explaining that

---

[103] Joint Statement on Data Protection and Privacy in the COVID-19 Response (2020), https://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response.

[104] Statement on the processing of personal data in the context of the COVID-19 outbreak (2020), https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[105] The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe recall the principles of data protection in these times of fight against the COVID-19 pandemic (2020), https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

the GDPR and Convention 108 do not hinder measures taken in the fight against the pandemic but require that emergency restrictions on freedoms will be proportionate and only valid during a limited emergency period. However, as governments continue to grapple with the devastating economic impact of the virus and prevention of its spread, it is likely that data privacy will remain undermined.

Future direction

Despite the public health challenges posed by the COVID-19 pandemic, the governments and private actors should not backtrack privacy principles that took us so long to develop.

We must thoroughly evaluate the possible trade-offs in using data during this crisis (the compromise between risks and benefits). Still, we must ensure that any outliers commensurate with the risks and are done with complete transparency, accountability, and a commitment to immediately stop or reverse the use of data outliers when the crisis ends.

Will governments restore the right to privacy when the danger is over? It remains to be seen, but based on the recent developments, paired with the public's growing readiness to compromise, we have all the more reasons to be skeptical.