İSTANBUL UNIVERSITY PRESS

Journal of Economy Culture and Society
JECS 2023; 68 : 46–59
DOI: 10.26650/JECS2023-1256957

Research Article

Digital Panopticon Dilemmas: A Study on Contact Tracing Apps Carried Out by the Ministry of Health

Elifnur TERZİOĞLU[1,2]

[1]Asst.Prof.Dr. Hatay Mustafa Kemal University Department of Radio, Television and Cinema, Faculty of Communication, Hatay, Türkiye.
[2]Atatürk University, Department of Public Relations and Publicity, Faculty of Communication, Erzurum Türkiye.

Corresponding author : Elifnur TERZİOĞLU
E-mail : elifnur.terzioglu@mku.edu.tr

ABSTRACT

Panopticon, often referred to alongside Michel Foucault and Jeremy Bentham, is a theory that explains the relationship between power and knowledge. Surveillance has gradually become a digital phenomenon as technology has developed, taking on a post-panopticon feature. Thus, it has become possible to monitor the entire flow of information. Although some individuals see this situation as a positive because it saves time and provides digital satisfaction, discussions around it mention that it restricts personal rights and freedoms in most societies. Although individuals voluntarily accept being watched in digital public spaces, they often forget that such surveillance will place them in some extraordinary situations that they might not agree with. During the Covid-19 pandemic, which affected the entire world, governments implemented some digital applications in order to track and manage their population. Through these applications, known as contact tracing systems, there was an attempt to control the spread of the illness. These systems used mobile phone applications to record personal data. This study analyzes 49 countries whose Ministries of Health applied contract tracing applications during the Covid-19 pandemic process through the digital panopticon perception, which would be labeled as classified data according to their democracy indexes.

Keywords: Digital Panopticon, Surveillance Cultures, Contact-tracing Apps, Covid-19

Submitted : 27.02.2023
Revision Requested : 25.05.2023
Last Revision Received : 25.07.2023
Accepted : 30.07.2023
Published Online : 20.11.2023

1. Introduction

The panopticon phenomenon emerged in 1785 with the prison model drawn by the English philosopher Jeremy Bentham, which was not able to be built at the time. The purpose of the panopticon, which includes a geometric structure and is defined as observing (opticon) the whole (pan), is to control the problems that may be experienced in a crowded human community. Throughout history, those who have held the power of government have constantly utilized a watchful element to control societies. With globalization, the phenomenon of surveillance, like many other elements, has undergone changes, has taken different forms, and has become one of the important power issues in our lives. People are now more curious about the lives of people of other societies, especially with the developments in technology, and want to follow global societal developments closely. For this reason, governments attempt to surveil others to protect their own people and themselves, especially during extraordinary situations. Surveillance, which is the basic form of power control, has easily spread to all areas of life with today's technological developments, forming an area of influence that even reaches the smallest social units. In addition, those in power are sometimes forced to take measures that will ensure the order and security of their societies, to maintain their existence, and to prevent unwanted behaviors. In doing so, they impose sanctions on their individuals, surveil them through the mass media, and thus attempt to establish a social order. Although the digitalization that occurs with technology is welcomed by many as a positive development, many believe that it restricts freedom. When looking at the issue critically, effective database use and management, the recording of electronic transactions, and the formation of an online tracking system has led to the emergence of a structure that observes everything done through information technologies, which may cause individuals to feel that their privacy is being violated. In today's world, where the digital environment is increasingly included in people's lives and the panopticon has shifted into a post-panopticon, the phenomenon of surveillance through the use of mass media has sometimes become a threat to fundamental rights and freedoms. The fact that most people unconsciously or voluntarily hand over their personal data to surveillants negatively affects not only their own privacy, but also social privacy through discrimination, marginalization, and fear. Personal data is stored by the power structures through digital surveillance and is used according to their need.

The source of motivation for this study is the feeling of being threatened in terms of privacy, rights, and freedom due to globalization and developments in communication technologies. The level of tolerance of individuals to this threat perception is expected to be higher due to the higher benefit they receive, despite privacy violations in health-related practices. As a matter of fact, in the study titled "*Contact tracing apps and values dilemmas: A privacy paradox in a neoliberal world*" written by Frantz Rowe in 2020, a qualitative study was conducted on whether contact tracing systems violate privacy. It was found that the access permissions requested for the applications violate privacy, but since it is a health application, people are more tolerant. In addition, Duan et al. (2022) investigated the privacy paradox in the adoption of contact tracing apps in Australia with a survey study titled "*Exploring privacy paradox in contact tracing apps adoption,*" which found that contact tracing systems have both benefits and risks.

Based on these studies, the present study examines 49 contact tracing applications which are thought to show higher tolerance because they are issued by the Ministries of Health. While studies on contact tracing practices exist in the literature, they generally do not go beyond a superficial examination of the practices of one or several countries. On the other hand, Bengio et al. descriptively discussed the privacy limitations of decentralized contact tracing systems in their study "*Inherent privacy limitations of decentralized contact tracing apps*". In the study "*Adoption of COVID-19 Contact Tracing Apps: A Balance Between Privacy and Effectiveness*" by Emily Seto et al. (2021), 11 applications from different countries were descriptively compared regarding the privacy and technological features of the respective COVID-19 contact tracing applications. In the article titled "*COVID-19 contact tracing apps: UK public perceptions*" by Samuel et al (2022), semi-structured interviews were conducted with practitioners on the privacy issue of COVID-19 contact tracing applications in the United Kingdom. In the study titled "*Privacy Analysis and Comparison of Pandemic Contact Tracing Apps*" by Piao and Cui, a comparison of centralized and decentralized contact tracing systems in terms of privacy was carried out. The study of Eismann et al. (2022) titled "*Applied Ethics and Digital Information Privacy: Informing the Design of Covid-19 Contact Tracing Apps*" is based on a descriptive comparison of the contact tracing practices of five liberal democracies.

The democracy comparison tool that Eismann et al. used in their study was further developed in this study, which investigates the contact tracing systems carried out by the Ministries of Health. They were classified according to the democracy indices of the countries and examined according to four classes, as: full democracy, flawed democracy, hybrid regime, and authoritarian regime. Through this distinction, more valuable outputs have been obtained. In this respect, this study makes a valuable contribution to the literature as it includes all original ministry practices.

2. Digitalization of Panopticon

In the 18th century, empires focused on authoritarian control systems in order to control the indigenous people. In 1785, Jeremy Bentham designed a structure to assist the power structures in terms of surveillance, which became a very valuable design for states that wanted to maintain control (Steadman, 2012). Throughout history, capitalist power has used the eye symbol as a sign of control over society, so that societies that are constantly under the control of the eye have been kept in a position where they cannot even attempt to do anything other than live in a state of constant surveillance. The concept of surveillance, which has changed according to social changes, has become the basic phenomenon of power and has brought human life into a prison-like system of order. The phenomenon of surveillance, which has spread to all areas of life, especially with the advancement of technology, restricts personal freedoms and attempts to control all areas of life by constantly recording what the citizens are doing. Although the panopticon is seen as an architectural structure, it has been stated that it is actually a form of management (Boyd & Crawford, 2012). When looking at the panopticon design, it has a ring-shaped architecture that allows surveillance, which means to observe (-opticon) the whole (pan-) and consists of single-chamber cells on several floors. Each cell opens to the inside of this ring, with a window present on the outer wall of the ring. In the middle of the ring is a guard tower where observers remain completely hidden from prisoners. The basic logic of the panopticon is that the one-room cell does not leave a hiding place for the prisoner, whereas the external light coming from the window of the outer wall allows the guards in the tower to watch a silhouette of the prisoner's every move. According to Bentham's approach, the prisoners in the observed position are people who know that every wrong behavior will result in punishment, however, they do not know when their behavior is actually observed so they have to act accordingly.

Foucault describes the panopticon as a phenomenon that is the basis of power and discipline, that today explains the authority of power over society (Mattelart, 2010) which makes its presence felt everywhere. The panopticon, which has a very strong influence on the discipline of societies, prevents the oblivion of power (Foucault & Meirelles, 2015). In this surveillance model, where privacy is not allowed because everything is under surveillance, the behavior of prisoners is put into a single pattern and discipline is ensured in this way. Prisoners who do not know how and when they are being surveilled, but know that they are being monitored, shape their attitudes and behaviors accordingly. Bentham expressed the panopticon as "a new model of a higher mind attaining power" (Bossewitch & Sinnreich, 2012). In fact, the concept of the panopticon is a surveillance system that goes beyond the metaphor of a prison. Foucault used this architectural structure as a metaphor for the modern surveillance society. Bentham's panopticon plan is based on the philosophy of asymmetrical surveillance. Asymmetric surveillance is based on not knowing when the person is being surveilled (Haggerty, 2006; Light, 2010). This practice of closure performs an effective function to enforce oversight more strongly and to provide the discipline that capitalism needs (Foucault, 1980a).

The panopticon, which consists of the prison project designed by Bentham in 1791, is a metaphorical concept used by Foucault to describe surveillance in modern society and is used in the sense of the spot directly in front of the eye (Oscar & Gandy, 1989). Bentham (2011) stated that this designed structure can be used for various purposes such as detention, isolation, forced labor, and training, and can also be adapted to different places, with the principle of invisible surveillance needing to be applied in order to achieve these objectives and conduct effective surveillance. Seeing without being seen reveals the main function of the surveillant. The feeling of constant surveillance in the space produces pressure and anxiety on the prisoners and shapes their behavior by maximizing their self-control (Bossewitch & Sinnreich, 2012). As can be seen in Figure 1, the classic panopticon is realized in a circular building. The perimeter of the round and domed structure is divided into cells with two windows. One is opening from the outside, allowing light to pass through, while the other is another window that opens towards the courtyard. In the center, in the courtyard section, there is a tower with windows opening towards the cells around it, and in the tower, there is a person in charge of surveilling the cells that are separated from each other and individualized. While each cell is constantly visible from the tower, and while the tower is visible from the cells, prisoners never know if they are actually being surveilled at a given time (Hamann, 2020; Safaei, 2020; Foucault, 1980b). In this way, it is possible for the surveillant to more easily establish authority over those who are monitored and to maintain this dominance.

Habermas (1992), one of the most important representatives of the Frankfurt School and critical theory, states that surveillance is intertwined with the private and public spheres in which we live and that this process strengthens the power of both the state and capital groups, which shapes the power relations in the new capitalist order. In the surveillance society, privacy becomes under threat, with information about all areas of both public and private life in danger of being presented to the ruling powers at any time. In his novel 1984, George Orwell (2003) focuses on the life of a totalitarian society trapped in a network of surveillance that monitors and records everything, surveilling the population at all times. Orwell draws attention to a social culture based on fear, oppression, and obedience, where thinking and acting against

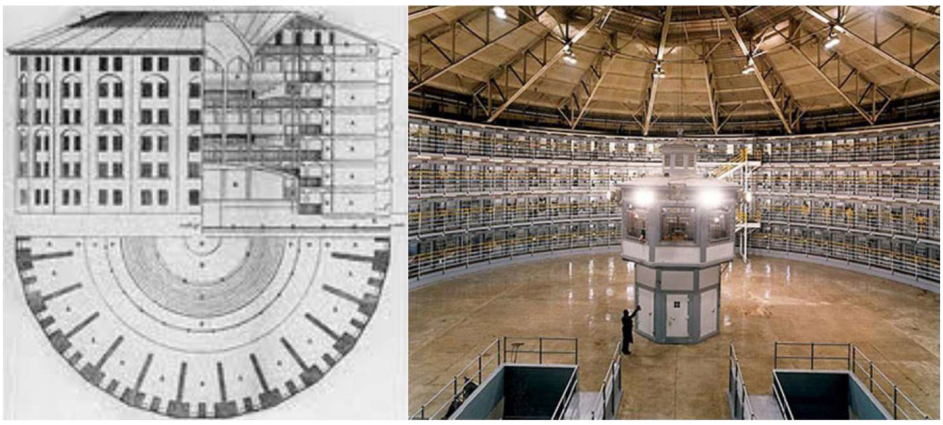

Figure 1. Architectural Design of Panopticon Source: Guardian, 2022

the power is considered a crime, with the "thought police" constantly surveilling and pressuring the population. Within the totalitarian social structure depicted by the novel, people are systematically, constantly, and forcibly surveilled in order to be kept under control. In recent years, with the accessibility provided by communication technologies, surveillance has been gradually spreading to a large part of society (Lyon, 1997). Especially in the capitalist order, the increasingly developing communication technologies facilitate surveillance practices in all dimensions and cause the continuity of control (Caluya, 2010).

The panopticon, which was put forward by Bentham and has gained depth in Foucault's discourse, has been very useful in understanding how the process of power works today. It is especially powerful in the modern age, when communication technologies are dominant, offering a solid framework to understand the world (Dobson & Fisher, 2007). In his book '*Panopticon*', Bentham defines surveillance as an unprecedented and new method of gaining power over the minds of individuals (Mattelart, 2010). The panopticon contains a constant state of visibility, where prisoners can be seen but cannot see. Accordingly, the panopticon represents an asymmetrical surveillance (Brivot & Gendron, 2011). According to Foucault, surveillance is involved in the whole of social life, from prisons to businesses, from schools to hospitals, resulting in an order in which the ruling power can establish its own hegemony (Sartori, 2017).

In line with the developments in today's communication technologies, individuals can be easily surveilled, not only in their working lives, but also in their private lives, with all kinds of information being recorded at any time through data banks and checked and inspected in every section of individuals' lives. Thus, it satisfies the desire for surveillance for those in power. Surveillance, which can enter all areas of social life, has thus reached the digital dimension, using individuals as part of the power structure. Therefore, wherever there is surveillance and control, the inevitable existence of power is confronted. Monitoring and surveillance activities are inherent components of control, including power and authority, and the surveillance society that emerges in the process also reproduces power relations. However, it is impossible to understand today's societies, where the boundary between the private and the public sphere is gradually disappearing and which continues to exist in a way depending on all surveillance systems, only with the concept of panopticon (Zuboff, 2019). Information and communication technologies digitize and globalize the concept of the panopticon and enable this concept to transform and change in cyberspace, leading to regeneration. Social media devices, and especially the widespread use of the internet, facilitate and make digital surveillance inevitable all over the world. This is explained by such concepts as: *superpanopticon* according to Poster (1990), liquid surveillance according to Bauman and Lyon (2012), digital siege according to Andrejevic (2007), and *post-panopticon* according to Boyne (2000). In fact, all of these and similar concepts, which derive from the panopticon, are used to explain the phenomenon of surveillance which is becoming increasingly globalized and digital, based on electronic dominance and voluntariness, and not by pressure, as is the case in the panopticon. Digitalization and a post-panopticon era have been prevailing in the modern age (Bauman & Lyon, 2012). Today's world is now based on voluntary surveillance practices rather than censorship and strict surveillance, with the voluntary form of surveillance attracting and persuading individuals (De Saulles & Horner, 2011). Surveillance based on volunteerism and consent, together with the development in communication technologies, enables the dissemination of information on a global scale without the limit of time and space and enables the internet and social networks to become widespread around the world. Although there are innovations in globalization, the concept of panopticon is now insufficient and evolving. It is seen that the panopticon became a synopticon which has become an omnipticon, which is the concept for defining consensual surveillance today.

In his 2004 book *The Naked Crowd*, Jeffrey Rosen introduces the concept of omnipticon, which was first used in the sense that everyone surveils each other, anytime and anywhere (Sprague, 2007). Today, the internet is a communication tool that allows most of the individuals to follow each other, and with the internet, the transition from the synopticon to the omnipticon concept has taken place. According to Rosen (2004), the omnipticon as a concept allows a majority of people, who do not know who is watching or being watched, to surveil each other at any time in the internet age. With this feature, the concept of omnipticon expresses everyone's mutual following each other in the digital environment and refers to a new social culture built on "voluntary surveillance," again based on the changing nature of surveillance practices. After the minority monitoring (synopticon), which expresses the transition from panopticon surveillance, where the surveillance of power remains at the local level, to a more global control and surveillance culture, together with the developing technology, the omnipticon stage, where everyone can monitor everyone else, has become realized (Pimenta, 2010). Through information communication technologies and social networks, everyone can now monitor, see, follow, and scrutinize everyone as they see fit. For this reason, although there are different practices in different countries of the world, there are laws in most countries for people to protect their data which have been developed in parallel with technology.

The Panopticon Foundation is a Poland-based organization founded in April 2009 with a mission to protect fundamental rights and freedoms against increased surveillance in parallel with changing technology (Panoptykon Foundation, 2022). While the omnipticon dimension of surveillance expressed here and the asymmetrical surveillance between power and the individual continues, symmetrical surveillance takes place between individuals. Today, the last point of surveillance based on voluntariness, entertainment, and individual consent, which replaces surveillance with coercion, pressure, and threat, is realized through the concept of omnipticon, which is the phenomenon of surveillance in the postmodern period. This transformation, on the other hand, contributes to the continuous reproduction of surveillance and the power relations attached to it by adapting it to the era. Communication technologies change and transform individuals as well as surveillance and power relations (Beniger, 1986). Countless volumes data is shared every second on the Internet, social networks, smart device applications, online services, and other digital media platforms. Although most of this data is shared voluntarily by the users, how this shared data is controlled is mostly unknown to them. Social listening is an active process that involves participating in, observing, interpreting, and responding to various environments through computer, electronic, and social channels (Stewart & Arnold, 2018).

3. Freedom and health against data privacy

Since the 1980s, in the period when the phenomenon of globalization gained a new dimension with neo-liberal policies, new communication technologies radically transformed almost every field from daily practices to social structures, from economic relations to political systems. This development has brought the need to redesign life in a digital way (Değirmenci, 2020). In the rapidly digitalizing world, everything is not provided by online application services. Without computers, mobile phones, and the internet, almost all services are incomplete. When considered historically, it is possible to say that humanity is better positioned to face infectious diseases today. In particular, the advancement of high-speed information exchange has a significant role in dealing with health problems (Alanka et al, 2022). The purpose of e-government applications, which provide more than 5000 different services, is to bring the entire government service online, to record the data of individuals, and to get to know them better so that they can provide better service. Government or commercial enterprises, which aim to easily reach individuals by having information about their tastes, tendencies, habits, and locations, generally follow the data recorded in social media applications in order to access this data. Traces left everywhere in the digital world hide information about people. Societies share and allow this data collected in the digital environment to be shared based on consent or without realizing it (Becker, 2019).

As seen in Figure 2, applications such as Facebook, Twitter, Yahoo, and LinkedIn stand out among the sites that have had the world's largest data breaches. Applications offering online government services, such as digital banking, social media accounts, online shopping, and mobile phone data, record all relevant data about the individuals, such as their age, education, job, income, and family information, as well as with whom, when, and where they spend time, using this information when necessary. Everything about a user can be accessed, including all the searches they make, which applications they open in which language, who they are speaking to and what they are saying on calls, location histories, and so much more (Ramageri, 2010). Some data is even sold to some companies. The recent example of this is the Cambridge Analytica scandal in the 2016 American elections. The scandal involves a data breach in which the personal information of 50 million Facebook users was collected (Nytimes, 2022). After this scandal, it can be said that people have started to have doubts about their data being recorded. Cameras placed in social areas, equipped with facial recognition systems supported by artificial intelligence which continuously follow individuals, are able reach people

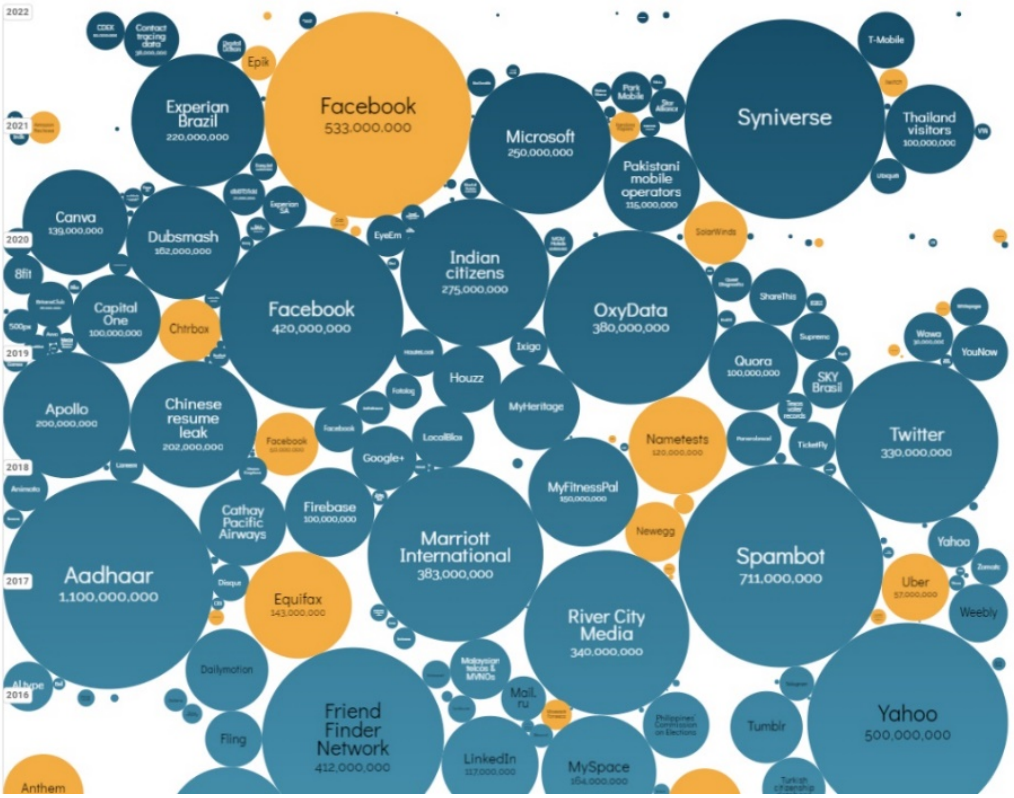

Figure 2. World's Biggest Data Breaches & HacksSource: Information is Beautiful, 2022

because of the tracking systems which have been implemented, allowing people's attitudes/perceptions to be altered in the desired direction (Nissenbaum, 1998). Orwell's sentiment in 1984 that "Big Brother is watching you!" is an adequate explanation of today's tracking systems (Literarydevices, 2022). After the Covid-19 outbreak, which affected the entire world, state authorities of every developed nation began taking measures to cope with this pandemic, so much so that everyone retreated to their homes for a period of time and started to comply with the social distancing rule. Those who did not comply with these measures were penalized (Moosa, 2020). Despite the growing fear of privacy, the pandemic revealed that people are willing to use these privacy-invading apps when it comes to health. It is expected that people's tolerance towards contact tracing applications is higher than their tolerance towards other applications. For this reason, many countries around the world developed contact tracing applications that were installed on smart phones to combat the novel coronavirus. The applications, which were first used in Asian countries such as China, South Korea, Singapore and Taiwan, were soon used all over the world (Kretzschmar et al, 2020). In order to control the number of cases, these practices were used to identify and inform people with positive test results the incubation period of the disease, warning them that they should isolate themselves from other people. Many authorities, hoping to take advantage of technological facilities to prevent the faster spread of the virus, pursued the development of such digital contact tracing systems. Despite concerns about the protection of personal data, governments prioritized minimizing the effects of the pandemic and preventing the spread of the disease (Eismann et al., 2022). Thanks to these applications during and after the Covid-19 process, the answers to questions such as who was contacted, how many times they met, and where and when they met became immediately available. Although these applications were developed to control the pandemic, concerns about privacy and data security breaches were real because they facilitate access to people's private data.

These monitoring system applications can be divided into two: centralized and decentralized (Martin et al., 2020). Although centralized and decentralized contact tracing applications vary according to countries, their common features are generally expressed as using Bluetooth technology in the mobile phone (WHO, 2021). With the data transfer between the two devices, the data of the individuals is collected and matched, revealing a map of disease risk. As a result, individuals could be warned about the precautions to be taken in case of risk detection. In the central system, the data of a person who tested positive for Covid-19 was recorded by their phone and transmitted to the center (Raskar et al., 2020). In the decentralized system, the people with whom the individual is in contact can only be seen from the person's own device, without being transmitted to the center. Individuals who are sensitive about privacy and personal

data security prefer the use of decentralized systems because unlike the centralized system, the data is made accessible to government institutions. In the decentralized system, although the governments' access to the data is limited, the pairings are made within the individual's own device. Therefore, the individual has more control over their data (Lv et al., 2022). In this area, where the issue of health comes to the forefront, most societies tolerate the privacy concern experienced due to the fact that the practices are carried out by the government.

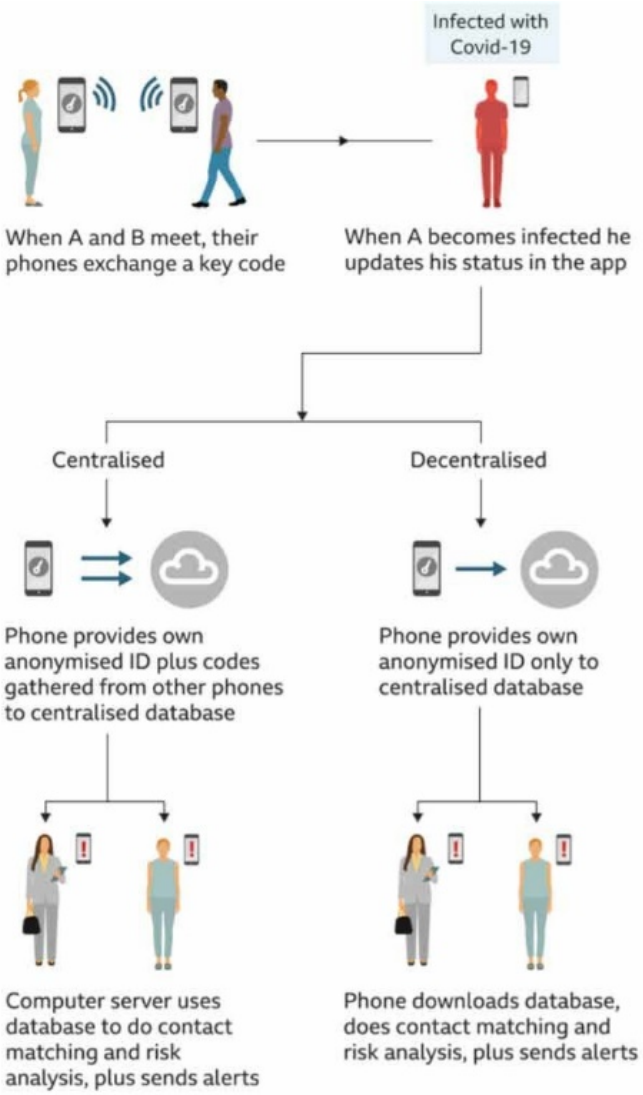

Figure 3. Centralized v. Decentralized systems Source: BBC, 2022

Contact tracing systems, which were designed as a precaution against the Covid-19 epidemic, also contain two opposite poles that touch on both privacy and public health (Rowe, 2018). In the centralized monitoring system application, recording the information of who is together with whom and for how long has caused the surveillance phenomenon to become popular again and even increase its impact on daily life (Sharon, 2020). The aim of these contact tracing practices is to warn people who interact with individuals who have tested positive. These applications use a centralized system that opens data to direct access and control by government agencies. In this way, it can impose restrictions on travel and public/social spaces. It was argued that, in order to prevent the spread of the Covid-19 virus, the distance between people is important, meaning that Bluetooth is the only sufficient way to measure this. However, applications using a centralized system provide access to various data from the phone, from the Global Positioning System (GPS) to the camera. When downloading applications, the user is asked for consent to access an incredible amount of personal data, including: a random anonymized user ID, address, age range, date of birth, device ID number, e-mail, gender, location, mobile number, name, nationality, passport ID, personal ID number, personal QR code, postcode, profile picture, pseudonymized, race, and ethnicity. The application is used not only to determine the social interaction of the

person with this data, but also to warn in case of contact with infected people and even direct the user to the relevant hospitals. Although it was argued that the more data that was recorded, the easier it would be to control the pandemic, valid criticisms stated such applications are a violation of privacy. Countries that adopted the decentralized method, such as Germany, Italy, Ireland, Austria, the United Kingdom, Spain, and Switzerland, stated that recording data would present a risk. Experts from these countries stated that the recording of a single location makes a person recognizable, while emphasizing that much of the recorded data would result in controversy about security (Parker, 2022). In the clarification text of the centralized contact tracing applications, the purposes of processing personal data are included in detail. Although the Covid-19 pandemic adversely affected the whole world and cost millions of people their lives, there is concern that such surveillance and monitoring practices lead to human rights and freedom of expression violations. In a fundamental sense, although it was affirmed that states struggled with the public health crisis, they still ignored the fundamental rights of their citizens, such as privacy and freedom of expression (Edri, 2022). The fact that individuals who felt that they were under constant surveillance during the pandemic remained more distant from others when they went outside emphasizes the authority of power that lies at the basis of the phenomenon of surveillance.

4. Methodology

The study was designed in a qualitative model, Netnography used as the data collection analysis method. Netnography is a fairly new methodology compared to traditional ethnography because it has only existed since the invention of the internet and is based on online observations, interviews, and content analysis of what is happening in digital environments. It can also be defined as a specific set of research practices related to data collection, analysis, research ethics, and representation based on researcher observation (Lee, 2020; Hookway, 2008). A case study was conducted about the research using the document analysis technique. It is stated that document review is a type of analysis that includes written sources containing information about the targeted facts and events and visual materials such as film, video, and photographs. The case study was conducted to describe one or more situations in depth and to draw attention to research questions and topics (Johnson and Christensen, 2014). Situations include critical events that take place in the lives of individuals, societies, institutions, and cultures (Hennink et al., 2020). In this context, the contact tracing systems used by governments to control the COVID-19 process have been examined in this study within the framework of the digital panopticon based on the democracy index published by the EIU in 2021. As a sample, 49 contact tracing applications collected from the Google Play Store, which were only used by the Ministries of Health of the selected countries, were examined based on the EIU's democracy index. In this context contact tracing applications used by governments designed to control the Covid-19 process have been categorized according to the desired information to be accessed from people who downloaded the applications to their mobile phones, ranking them according to the democracy index, highlighting the importance of personal data privacy for each country in question.

5. Democracy Index and Contact Tracing Applications

The UK-based Economist Intelligence Unit (EIU) has been preparing the Democracy Index every year since 2006. This democracy index aims to measure the democratic position of 167 countries (EIU, 2022). The EIU's democracy index is grouped into five categories: electoral process and pluralism, civil liberties, state functions, political participation, and political culture. These categories are based on the rating of a total of 60 indicators. Each category consists of a rating between 0 and 10 (Rahman, 2014).

According to this report, there are four different regime systems between countries. The first of these are *Full democracies*, which are countries that respect not only civil liberties and fundamental political freedoms but also the development of democratic principles, even supported by political culture. These countries face few problems, with balanced government systems, independent judicial systems, independent media, in short, adequately functioning governments (Populismstudies, 2022). In *flawed democracies*, although elections are held freely and fairly, they are still more likely to encounter problems than in fully democratic countries. They may face such problems as violations of media freedom and the possibility of suppression of opposition parties. They also have deficiencies in other democratic dimensions, including underdeveloped political culture, low levels of participation in politics, and issues in the functioning of governance (Populismstudies, 2022). *Hybrid regimes* consist of countries with unfair elections and a structure that restricts freedom. These countries often have more obvious faults than flawed democracies in areas such as weak political opposition, non-independent judiciary, rampant corruption, and harassment and repression of the media (Menocala et al, 2008). *Authoritarian regimes* are countries where political pluralism has disappeared or is extremely limited. While these countries often have absolute monarchies or dictatorships, violations and abuses of civil liberties are common, elections (if they happen) are not fair and free, the media is often controlled by the ruling

regime in power, the judiciary is not independent, and censorship and government criticism prevail everywhere (Linz et al., 2000).

The contact tracing applications used by the Ministries of Health of the 49 countries subject to the study have been categorized in terms of what personal data the applications require while using them and the four regime systems according to the democracy index. The results of this categorization are provided in Table 1.

Table 1. Index score, ranking, and TurkStat values in the domain of civic participation for Turkey

TYPE OF REGIME	COUNTRY	Democracy Indexes	Personal Identity														
			A RANDOM USER ID	ADDRESS	AGE RANGE	DATE OF BIRTH	DEVICE&PERSONEL& PASSPORT ID NUMBER	E-MAIL	GENDER	LOCATION	MOBILE NUMBER	PSEUDONYMİSED	NATIONALITY	PERSONAL QR CODE	POSTCODE	PROFILE PICTURE
Full Democracies	New Zealand NZ COVID Tracer	9,97					x				x					
	Norway Smittestopp	9,75														
	Finland Koronavilkku	9,27														
	Sweden COVID Symptom Study	9,26		x				x				x				
	Denmark Smitte|stop	9,09								x						
	Ireland COVID Tracker Ireland	9														
	Taiwan Taiwan Social Distancing	8,99														
	Australia COVIDSafe	8,9			x					x	x	x			x	
	Switzerland SwissCovid	8,9					x									
	Netherlands CoronaMelder	8,88														
	Canada Covid Alert	8,87					x			x		x				
	Luxembourg CovidCheck.lu	8,68														
	Germany Corona-Warn-App	8,67														
	South Korea Self-Diagnosis app	8,16			x				x	x						
	Japan COVID-19 Contact-Confirming	8,15														
	Austria StopCorona	8,07									x	x				
Flawed	France TousAntiCovid	7,99								x						
	Israel Hamagen	7,97								x						
	Spain Radar COVID	7,94	x													
	Portugal STAYAWAY COVID	7,82	x													
	Czech RepublicıeRouška	7,74		x			x									
	Italy SM-COVID-19	7,68								x						
	Malta COVID Alert Malta	7,57									x					
	Greece DOCANDU Covid Checker	7,56		x				x	x		x	x				

Table 1 . Continued

	Slovenia #Ostanizdrav	7,54			x			x	x		x	x						
	Belgium Coronalert	7,51		x							x	x	x					
	Cyprus CovTracer	7,43										x						
	Malaysia MySejahtera	7,24		x		x	x	x	x			x	x					
	South Africa COVID Alert South Africa	7,05						x		x	x	x						
	India Aarogya Setu	6,91						x		x	x	x						
	Brazil Coronavírus - SUS	6,86								x	x	x						
	Poland ProteGO Safe	6,8																
	Indonesia PeduliLindungi	6,71		x					x	x		x						
	Bulgaria ViruSafe	6,64			x		x			x		x						
	Singapore TraceTogether	6,23	x								x							

TYPE OF REGIME	COUNTRY	Democracy Indexes	Personal Identity															
			ADDRESS	AGE RANGE	DATE OF BIRTH	DEVICE&PERSONEL &	E-MAIL	GENDER	LOCATION	MOBILE NUMBER	PSEUDONYMİSED	NATIONALITY	PERSONAL QR CODE	POSTCODE	PROFILE PICTURE	RACE&ETNICITY
Hybrid Regimes	Bangladesh Corona Tracer BD & Surokkh	5,99				x			x							
	Bhutan Druk Trace	5,71				x		x	x	x	x					
	Hong Kong LeaveHomeSafe	5,6								x	x					
	Turkey HES Code	4,35							x	x						
	Pakistan COVID-19 Gov PK	4,31							x	x						
Authoritarian Regimes	Kuwait Shlonik	3,91				x			x	x						
	Qatar EHTERAZ	3,65							x							
	Russia StopCoronaVirus My Contacts	3,24				x				x						
	Kazakhstan Ashyq	3,08				x				x						
	Vietnam PC-Covid	2,94											x			
	Bahrain BeAware Bahrain	2,52						x	x	x	x					
	China Health Code	2,21				x		x			x				x	
	Uzbekistan Self-Safety	2,12			x	x										
	Iran AC19	1,95		x					x	x	x					

Discussion and Conclusion

Surveillance is a phenomenon that has been a necessity of gaining control and power throughout history. There are many studies on surveillance and surveilling, the most important of which is the concept of the panopticon. Surveillance studies have become diversified and enriched with the constant advancement of technology. Many factors constitute a source for studies on the panopticon, such as: globalization, the diversity of communication tools and communication forms, the changes occurring in the social and economic balances in the world, and power wars. Surveillance has not disappeared in the modern age, which can be described as the post-panoptic age. On the contrary, it has become more and more involved in the lives of today's people in various forms. Closed system cameras, biometrics, smart objects, cloud computing, blockchain, and, of course, social media have become post-panoptic surveillance tools. Many people use new technologies, either out of necessity or voluntarily. Especially after the developments in communication technologies, the general public use the new media quite comfortably and do not hesitate to disclose their private lives. People often gladly and voluntarily accept the products or services offered to them by the new media and do not hesitate to share their personal information with product and service providers. Surveillance has evolved to be virtual and data-oriented, while it was previously done physically, preferably in closed environments. Data obtained from digital applications is important for many companies and governments. Thanks to digital applications described as data banks, system administrators who can now easily access all personal data can intervene in incidents at any time and situation. The recent example of this is the Covid-19 pandemic. In today's world where data abundance is experienced, states developed contact tracing systems to prevent the spread of the Covid-19 pandemic. In this context, they attempted to determine where, when, and with whom the population was at all time by accessing people's data.

As we move from full democracy to authoritarian regimes, the perception that respect for the privacy of personal data will decrease and that there will be more desire to access data is expected. As can be seen in Table 1, when full democracies and flawed democracies are compared, there is an increase in the type of data requested to be accessed in the direction of flawed democracies, except in the case of Australia. Likewise, when compared to full democracies, the access permissions requested by hybrid and authoritarian regimes for contact tracing applications are quite high.

The personal data requested for access to contact tracing practices in flawed democracy countries is similar to the data that hybrid and authoritarian regimes requested access to, with there being no significant difference between full democracies and flawed democracies that can be observed. One of the reasons for this is the belief that certain access requests are necessary in order to achieve the purposes that contact tracing applications serve.

Norway, Finland, Ireland, Taiwan, the Netherlands, Luxembourg, Germany, and Japan did request access to personal data for contact tracing applications. They can be seen as countries that pay maximum attention to personal privacy. Although Australia is a fully democratic country, it surprisingly requested access to far more personal data than similar countries in the democracy index.

Although Poland is among the flawed democracy countries, it did not request permission to access any personal data, keeping personal privacy at the maximum level. France, Israel, Spain, Portugal, Malta, and Cyprus, on the other hand, displayed high levels of respect for personal privacy according to their own classification and even better than a few of the full democracy countries.

The contact tracing applications requests for access to personal data for Qatar and Vietnam do not comply with the characteristics of the authoritarian regimes in which they are classified. Contrary to expectations, they requested minimal access to personal data.

This study aimed to make a classification of contact tracing applications in terms of personal privacy according to country characteristics. It can be said that there is a serious difference between the way societies normally look at the requests to access personal data in any social application and the perspective of the personal data requested by the applications related to this field when it comes to health. However, some countries with full democracies and flawed democracies acted sensitively despite the issue of health, paying great attention to personal data privacy. The study is unique as it compares contact tracing systems applied only by the Ministry of Health of the examined countries according to the democracy index, which is an acceptable classification. In this way, it has also made an important contribution to the literature. In our next study, high-level quantitative methods will be used in conjunction with data to be obtained from surveys conducted on application users by classifying the countries of these users according to their different characteristics. The comparative results of this study will be examined, and thus, more valuable outputs will be obtained.

Ethics Committee Approval: Available online and publicly available report data were used, and the secondary data mentioned in the article complies with the ethical standards in Turkiye.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The authors have no conflict of interest to declare.

Grant Support: The authors declared that this study has received no financial support.

ORCID :

Elifnur TERZİOĞLU 0000-0002-3467-1537

REFERENCES

Alanka, Ö., Çimen, Ü., & Değirmenci, F. (2022). Cyberchondria as Digital Psychopathology: Covid 19 Pandemic Example. *Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (56), 185-202.

Bauman, Z. & Lyon, D. (2012). Liquid Surveillance: A Conversation. Cambridge: *Polity Publications.*

Becker, M. (2019). Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology, 21*(4). 307–317, https://doi.org/10.1007/s10676-019-09508-z

Bengio, Y., Ippolito, D., Janda, R., Jarvie, M., Prud'homme, B., Rousseau,J., Sharma, A., Yu, Y. (2021). Inherent privacy limitations of decentralized contact tracing apps. *Journal of the American Medical Informatics Association,* (28)1,193–195, https://doi.org/10.1093/jamia/ocaa153

Beniger, JR. (1986). The Control Revolution: Technological and Economic Origins of the Information Society. *Harvard University Press*.

Bentham, J. (2011). The panopticon writings. *Verso Books.*

Big Brother is Watching You. Retrieved from https://literarydevices,net/big-brother-is- watching-you/ Accessed 28.06.2022

Bossewitch, J. & Sinnreich, A. (2012). The end of forgetting: Strategic agency beyond the panopticon. *New Media & Society, 15* (2).

Boyd, D. & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*. 15(5): 662–679.

Boyne, R. (2000). Post-Panopticism. *Economy and Society*, (29)2.

Brivot, M. & Gendron, Y. (2011). Beyond panopticism: On the ramifications of surveillance in a contemporary professional setting. *Accounting, Organizations and Society*, (36).

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. Social Identities, (16).

Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html Accessed 28.06.2022

Covid-19 Apps. Google Play, Playstore. https://play.google.com/store Accessed 11.10.2022

De Saulles, M. & Horner, D.S. (2011). The portable panopticon: Morality and mobile technologies. Journal of Information, Communication and Ethics in Society.

Değirmenci, F. (2020). The Digitalization of Politics: The New Communication Devices and the Issue of Political Participation. in M. S. Erciş & E. E. Başar (ed,). *New Communication Approaches in the Digitalized World, Newcastle upon Tyne: Cambridge Scholars Publishing*, 273-288.

Democracy Index 2021: The China Challenge. Retrieved from https://www,eiu,com/n/campaigns/democracy-index-2021/ Accessed 21.11.2022

Dobson, J. E. & Fisher, P. F. (2007). The panopticon's changing geography. *Geographical Review, 97*(3), 307–323, doi: 10,1111/j.1931-0846.2007.tb00508.x

Duan, S. X. & Deng, H. (2022). Exploring privacy paradox in contact tracing apps adoption. *Internet Research.*

Edri, (2021). EDRis interactive Annual Report: A year in review of the digital rights field. Retrieved from https://edri,org/our-work/edris-interactive-annual-report-a-year-in-review-of-the-digital-rights-field/ Accessed 28.06.2022

Eismann, K., Fischer-Preßler, D., & Fischbach, K. (2022). Applied Ethics and Digital Information Privacy: Informing the Design of Covid-19 Contact Tracing Apps. *Australasian Journal of Information Systems, 26*, https://doi.org/10.3127/ajis.v26i0.3097

Flawed/Defective Democracy. Retrieved from https://www,populismstudies,org/Vocabulary/flawed-defective-democracy/ Accessed 15.11.2022

Foucault Welles, B. & Meirelles, I. (2015). Visualizing computational social science: The multiple lives of a complex image. *Science Communication*, 37(1): 34–58.

Foucault, M. (1980a). Power/Knowledge: Selected Interviews and Other Writings 1972–1977. London: Harvester Press, 98.

Foucault, M. (1980b). The Eye of Power, in C, Gordon (ed.). Power/Knowledge, Brighton: Harvester, 147–165.

Full Democracy. Retrieved from https://www,populismstudies,org/Vocabulary/fulldemocracy/Access Date 15.11.2022

Habermas, J. (1992). The Structural Transformation of the Public Sphere: Inquiry into a Category of Bourgeois Society. *Polity Press.*

Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon, in Lyon, D, (Ed,), Theorizing surveillance, Willan.

Hamann, J. (2020). Governance by Numbers: A Panopticon Reversed?. *Politics and Governance, 8* (2).

Hennink, M., Hutter, I., & Bailey, A. (2020). Qualitative research methods. Sage.

Hookway, N. (2008). Entering the blogosphere': some strategies for using blogs in social research. *Qualitative Research,* (8)1, 91-113.

Johnson, B. & Christensen, L. (2014). Educational Research: Quantitative, Qualitative, and Mixed Approaches. Fifth Edition, *Sage Publications.*

Kelion, L. (2020). Coronavirus: Contact-tracing apps face further hitches. Retrieved from https://www.bbc.com/news/technology-53051783 Accessed 28.06.2022

Kretzschmar M. (2020). Impact of delays on effectiveness of contact tracing strategies for COVID-19: a modelling study. *The Lancet Public Health*, (5)8,e452-e459, ISSN 2468-2667, https://doi.org/10.1016/S2468-2667(20)30157-2

Lee, C. S. (2021). Contact tracing apps for self-quarantine in South Korea: rethinking datafication and dataveillance in the COVID-19 age. *Online Information Review*, (45)4, 810-829.

Light, A. (2010). The Panopticon reaches within: how digital technology turns us inside out. *IDIS* 3, 583–598, https://doi.org/10.1007/s12394-010-0066-7

Linz, J. J. & Linz, J. J. (2000). Totalitarian and authoritarian regimes. *Lynne Rienner Publishers.*

Lv A., Luo T. & Duckett, J. (2022). Centralization vs, Decentralization in COVID-19 Responses: Lessons from China. *J Health Polit Policy Law,*1;47(3):411-427, doi: 10.1215/03616878-9626908, PMID: 34847219.

Lyon, D. (1993). An Electronic Panopticon? A Sociological Critique of Surveillance Theory. *The Sociological Review, 41*(4):653-678, doi:10.1111/j.1467-954X.1993.tb00896.x

Martin, T., Karopoulos, G., Hernández-Ramos, J., Kambourakis, G., Fovino, I. (2020). Demystifying COVID-19 digital contact tracing: a survey on frameworks and mobile apps. arXivcs 2020, doi: 10.1155/2020/8851429.

Mattelart, A. (2010). The Globalization of Surveillance: The Origin of the Securitarian Order 1st Edition, *Polity.*

Menocala, A. R., Fritzb, V., Raknerc, L. (2008). Hybrid regimes and the challenges of deepening and sustaining democracy in developing countries. *South African Journal of International Affairs. 15*(1):29-40.

Moosa, I. A. (2020). The effectiveness of social distancing in containing Covid-19. Applied economics.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public, Law and Philosophy.17(5/6), 559, https://doi.org/10.2307/3505189

Orwell, G. (2003). 1984. (N, Akgören, Trans,), *Can Publish*. (5).

Oscar, H. & Gandy, Jr. (1989). The Surveillance Society: Information Technology and Bureaucratic Social Control, *Journal of Communication.* (39)3, 61–76, https://doi.org/10.1111/j.1460-2466.1989.tb01040.x.

Panoptykon Foundation. Retrieved from https://panoptykon.org/ Accessed 27.06.2022

Parker, M. C., Fraser, L., Abeler-Dorner, and Bonsall, D. (2020). The ethics of instantaneous contract tracing using mobile phone apps in the control of COVID-19 pandemics. https://github,com/BDIPATHOGENs/covid-19_instant_tracing/blob/master/ The ethics of instantaneous contract tracing using mobile phone apps in the control of pandemics, pdf, Accessed 19.09.2022

Piao, Y. & Cui, D. (2021). Privacy Analysis and Comparison of Pandemic Contact Tracing Apps. KSII Transactions on Internet and Information Systems, 15, 11, (2021), 4145-4162.doi: 10.3837/tiis.2021.11.015.

Pimenta, E. D. M. (2010). The city of sun: panopticon, synopticon and omniopticon-big brother and the giant with thousand eyes, In Pimenta, E, D, M, (Eds,), Low power society- continuous hyperconsumption and the end of the medium class in a hyperurban planet UK: *ASA Art and Technology Limited* ,260-303.

Poster, M. (1990). The Mode of Information: Poststructuralism and Social Context. *University of Chicago Press.*

Rahman, M. S. (2014). Statistical analysis of democracy index. *Humanomics* 30(4):373-384.

Ramageri, B. M. (2010). Data mining techniques and applications. Indian Journal of Computer *Science and Engineering.* (1)4, .301-305.

Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., et al. (2020). Apps gone rogue: maintaining personal privacy in an epidemic. arXivcs 2020

Rosen, J. (2004). The Naked Crowd Reclaiming Security and Freedom in an Anxious Age. *Random House Inc.*

Rowe, F. (2018). Being critical is good, but better with philosophy! From digital trans- formation and values to the future of IS research. *European Journal of Information Systems, 27*(3), 380–393.

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neoliberal world. *International Journal of Information Management, 55*, Article 102178.

Safaei, S. (2020). Foucault's Bentham: Fact or Fiction?. International Journal of Politics, Culture, and Society. Retrieved from https://link.springer.com/content/pdf/10.1007/s10767-019-09342-7.pdf

Samuel, G., Roberts, S. L., Fiske, A., Lucivero, F., McLennan, S., Phillips, A., Hayes S. & Johnson, S.B. (2022). COVID-19 contact tracing apps: UK public perceptions. *Critical Public Health*, 32:1, 31-43, DOI: 10.1080/09581596.2021.1909707

Sartori, G. (2017). The Transformative Power of Near-Death Experiences: How the Messages of NDEs Can Positively Impact the World. *Watkins Publishing.*

Seto, E., Challa, P., Ware, P. (2021). Adoption of COVID-19 Contact Tracing Apps: A Balance Between Privacy and Effectiveness. *J Med Internet Res*, 23(3):e25726.

Sharon, T. (2020). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology,* 1–13.

Sprague, R. D. (2007). From Taylorism to the omnipticon: expanding employee surveillance beyond the workplace. *Journal of Computer &*

Information Law, 25 (1), 1-35.
Steadman, P. (2012). Samuel Bentham's panopticon. *Journal of Bentham Studies, 14*(1), 1–30.
WHO. (2021). Contact tracing in the context of COVID-19: Interim Guidance. 6-9.

How cite this article

Terzioglu, E. (2023). Digital panopticon dilemmas: A study on contact tracing apps carried out by the ministry of health. *Journal of Economy Culture and Society, 68,* 46-59. https://doi.org/10.26650/JECS2023-1256957