IAPA 2022
IAPA 2022 International Conference and International Indonesia Conference on Interdisiplinary Studies (IICIS)
Volume 2023

Research Article

Public Security vs Personal Privacy: Analysis of PeduliLindungi from Open Government and Surveillance State Perspectives

Sri Harjanto Adi Pamungkas*, Khusnul Prasetyo, Bhakti Gusti Walinegoro

Department of Public Policy and Management, Faculty of Social and Political Sciences, Universitas Gadjah Mada, Yogyakarta, Indonesia

Abstract.
The COVID-19 pandemic has driven the development of the implementation of surveillance states in various countries worldwide. As various countries go all out to control the spread of the pandemic, the central pillar used in controlling the pandemic is tracking social mobility and collecting citizen data on a massive scale. The development of digital surveillance during the COVID-19 pandemic has increasingly heated the debate regarding the dilemma between public security and citizens' privacy. Indonesia's PeduliLindungi is a mobile phone application that played a central role as the instrument for pandemic surveillance. This study aims to analyze PeduliLindungi as the object of research. The analysis focuses on whether PeduliLindungi is more likely based on the principles of open government or surveillance state. This study concludes that when viewed based on the features of the PeduliLindungi application, the terms and conditions of use of the application, to the privacy policy applied by the PeduliLindungi application, the PeduliLindungi application is more oriented toward open government rather than a surveillance state.

Keywords: pandemic COVID-19, public security, personal privacy, PeduliLindungi, open government, surveillance state

Corresponding Author: Sri Harjanto Adi Pamungkas; email: sri.harjanto.adi.pamungkas@mail.ugm.ac.id

Published 6 March 2023

Publishing services provided by Knowledge E

© Sri Harjanto Adi Pamungkas et al. This article is distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use and redistribution provided that the original author and source are credited.

Selection and Peer-review under the responsibility of the IAPA 2022 Conference Committee.

OPEN ACCESS

1. Introduction

1.1. The Emergence of e-Government and Digital Governance

Governments in the world today face dynamics generated by the influence of technological advancements. The presence of mass production technology applied to manufacturing has resulted in the post-industrial economy of mass production since the 1950s. Subsequently, the presence of the internet in the 1990s brought the world to a new phase, namely the knowledge-based economy. It was followed shortly by the development of digital technology in the 2000s, which brought the world into the era of digitization.

The latest developments from the latest advanced technologies, such as the internet of things, cyber-physical systems, advanced robotics, and new materials, have brought the world into the fourth-generation industrial period [1]. This development creates a giant and integrated digital ecosystem consists of e-commerce, e-business, e-learning, e-media, and e-government [2].

Specifically in the public sector, the emergence of e-government has become a new chapter of government practice and public policy for countries worldwide. E-government is the embryo of digital-based governance as a further adoption of technology entry into the public sector. Enthusiasm for implementing digital governance is continued by the top-down encouragement from various international institutions such as the United Nations, ADB, World Bank, and IMF. The Emergence of social media also strengthens this dynamic as a new public space that allows decentralized public discourse [3]. This new public space becomes a bridge that brings bottom-up aspirations from the community regarding open, real-time, and digitally integrated governance. The combination between top-down pressures and bottom-up aspirations provides the impetus for countries in the world to transform towards digital governance.

Furthermore, many experts, mainly from the field of sociology, state that currently is the starting point of a post-bureaucratic era [4, 5]. This is indicated by the tendency of organizations in both the public and private sectors to become more horizontal and efficient [6]. This phenomenon manifests a more democratic relationship between the state and its citizens. However, it must be acknowledged that there are differences in the speed of adaptation to this changing trend. For example, OECD member countries are at the forefront. While developing and underdeveloped countries are still in the practice of the Weberian bureaucracy.

There are at least three characteristics of this horizontal and efficient post-bureaucratic era. The first is the streamlining of bureaucratic procedures due to information technology. Activities such as licensing and investment can be done 100 percent digitally. The second is creating a control mechanism over the government through social media. Currently, social movements, petitions, and policy advocacy that can change political order and public policy are mostly done through social media. The third is the increasingly widespread application of digital governance throughout the world. Welchman states that organizations in both the public and private sectors adapt go-digital approaches to increase accountability and encourage better policy-making [7]. Furthermore, the same study identified various instruments used, including websites, mobile sites, social media channels, and other web-enabled products and services.

Countries deliver initiatives through available public policy instruments to transform toward digital governance. Interestingly, the results and impacts differ [8]. For example, digital governance in China tends to lean in the practice of surveillance state, while in Estonia, it tends to lean in the practice of open government. This is certainly interesting to analyze by bringing up a fundamental question, ”why do countries with the same vision of building digital governance produce different results and impacts?”.

1.2. Digital Governance: Open government vs. Surveillance State

The main question regarding the phenomenon described in the previous paragraph is, ”is the impact of this increasingly digitized post-bureaucratic era always uniform and positive for every country?”. This question needs to be answered with a theoretical analysis before being answered with a practical analysis of the existing cases. The first thing that needs to be done in answering this theoretical question is to know the value creation framework in this post-bureaucratic era. In simple terms, there are inputs, processes, and outputs (the use of outputs in this analysis includes outcomes and impacts). The input, in this case, is technological instruments, especially digital-based technology. In this case, the process is public policies delivered to manage the use of technological instruments (inputs). Finally, the output, in this case, is the resulting impact on citizens.

In terms of input, in general, countries around the world use relatively uniform technology. This is because the technology sector, significantly advanced technology, is semi-monopolistic. For example, semiconductor production is controlled by Taiwan, South Korea, and Japan. At the same time, the semiconductor license is controlled by the United States. Meanwhile, the latest generation of broadband networks, namely 5G, is monopolized by China through Huawei. Then artificial intelligence (AI) technology is also dominated by the United States and China. Lastly, technology and production licenses are also controlled by the United States, China, South Korea, and Germany for the internet of things. Therefore, the technologies used as inputs in the digital governance ecosystem are uniform. Countries worldwide import these technologies from a few sources: the United States, China, South Korea, Japan, and Germany.

If the input is uniform, is the process used also uniform? The answer to this question turns out to be no. There are two streams of policy as processes in digital governance. The first stream is a process that encourages the creation of open government. This is done by a country issuing a policy to encourage the digitization of information and public services in a democratic way. The second stream is a process that encourages

the creation of social, economic, and political stability. This is done by a country issuing a policy to encourage complete supervision and censorship of its citizens.

If there are two policy streams in the process, are the outputs (starting with the word impact) produced uniform or varied? Looking deeply at the current trend, there are two types of countries in digital governance. The first type is a country that can be called an open government. This type of country is where the government has thoroughly digitized public information and public services through digitization. This allows citizens to access public information without the need to go through bureaucratic procedures. Citizens only need to use the internet because various public information is available on government websites. In addition, citizens can also enjoy access to public services digitally.

On a practical level, Estonia is a country that represents the open government category. Estonia builds collaborative digital governance called e-Estonia, which builds on three actors. The three actors are referred to as (1) Forward-thinking Government, (2) Proactive Private IT Sector, and (3) Switch-on, Tech-savvy Population. Kalvet states that e-Estonia can be successful because the government continues to encourage public procurement for innovation activities [9]. Kitsing states that the private sector also plays an essential role because it proactively builds an internet-based banking system which later becomes the basis for the development of e-Estonia [10]. Sai & Boadi state that the existence of a community with high technological literacy supported by an advanced education system contributes to the success of the open government in Estonia [11].

Meanwhile, the second type is a state called a surveillance state. This type of country is a country that, through digitization of government, conducts supervision and censorship of the activities of citizens. Furthermore, surveillance and censorship are also carried out on the activities of foreigners currently in a surveillance state. Marx defines this digital surveillance activity as ”the act of real-time and retrospective viewing, processing and cataloging of online footprints against the will and/or knowledge of the actor(s) to whom such data belongs” [12].

On a practical level, China is a country that represents the surveillance state category. Interestingly, the embryo of the surveillance state in China started by digitizing forensic medical data in the early 2000s. Dirks & Leibold states that the successful digitization of forensic medical data named the Nationwide Y-STR Database was then continued in several areas with expansion on a national scale [13]. China then expanded its surveillance state practice through a social credit system program. Hoffman, in his study, states that the Chinese government, through the social credit system, has explicitly

expanded political control over citizens [14]. This social credit system collects analyzed citizen data to monitor and regulate citizen behavior.

1.3. The COVID-19 Pandemic and the Development of Digital Surveillance

The COVID-19 pandemic has driven the development of the implementation of surveillance states in various countries in the world. This is because various countries are trying their best to control the spread of the pandemic. The central pillar in controlling the pandemic is tracking social mobility and collecting citizen data on a massive scale. In this context, conducting digital surveillance is a very effective instrument in controlling the pandemic and especially considering that the pandemic presents various structural challenges [15]. The pandemic has caused various production sectors to experience shocks [16]. This causes economic productivity to decrease significantly. As a result, in 2020, the world economy will experience a 3.9 percent contraction, leading to the loss of 255 million full-time jobs and the emergence of 119 to 124 million new poor people [17].

China, South Korea, Hong Kong, and Israel built extensive digital surveillance systems during the COVID-19 pandemic. Israel uses digital technology to monitor the location of citizens infected with COVID-19, mainly during the 14-day quarantine period. South Korea uses smart city infrastructure (credit cards, cell phones, and CCTV cameras) to track the movements of citizens infected with COVID-19. China uses facial scanning and cell phone tracking technology for citizen surveillance and drones for quarantine discipline enforcement. Hong Kong uses innovative technology linked to mobile phone applications that can track citizens' movements.

1.4. PeduliLindungi

Indonesia has also taken digital surveillance initiatives in handling the COVID-19 pandemic through PeduliLindungi. PeduliLindungi launched as a mobile phone application. PeduliLindungi is a policy instrument used by the Indonesian government in tracking social mobility and monitoring potential virus outbreaks against citizens. PeduliLindungi is also an instrument for enforcing quarantine discipline as well as telemedicine platform. Further development of PeduliLindungi is directed to become a tracing system integrated with various modes of travel and access to public facilities. PeduliLindungi is also integrated with the vaccination program and citizenship identity, namely identity card

(KTP). The presence of PeduliLindungi as a digital surveillance instrument in Indonesia has also brought Indonesia into a vortex of debate regarding public security and citizen privacy. The question then arises, ”Does PeduliLindungi tend to be closer to the practice of open government or surveillance state?”

1.5. Problem Formulation

The development of digital surveillance during the COVID-19 pandemic has increasingly heated the debate regarding the dilemma between public security and citizens' privacy. On the one hand, pro-surveillance groups emphasize attention to the importance of government digital surveillance on citizens to maintain public stability. On the other hand, pro-privacy groups pay attention to the importance of upholding citizens' privacy rights. Public opinion is divided into these two blocks [18]. During the pandemic, the debate grew between groups of medical personnel and privacy & civil rights advocates [19]. The group of medical personnel urged the widespread increase in digital surveillance to deal with the pandemic. Privacy and civil rights advocate groups reject the agenda of expanding digital surveillance because it violates citizens' privacy rights.

This study aims to analyze PeduliLindungi as the object of research. The analysis focuses on whether PeduliLindungi is more likely based on the principles of open government or surveillance state. More specifically, this research will examine whether PeduliLindungi focuses more on achieving public security through pandemic control or on achieving digital democracy in pandemic control based on protecting citizens' privacy. Therefore, this research will be based on two main theories as analytical instruments, namely open government, which is connected to the concept of privacy, and surveillance state, which is connected to the concept of public security.

2. Literature Review

2.1. Open Government

Open government has become a digital governance concept that has received wide attention as technology advances. The concept of open government can be traced back to the 1950s. Open government, in its development is highly related with ideas about public information, transparency, accountability, participation, and collaboration [20]. Open government is a 'hallmark' of modern democracy [21]. This is because the

concept of open government brings the idea of accountability of public officials to citizens through the provision of public information.

Open government has many definitions but is connected to the same basic idea. Open government uses information technology to encourage participatory and collaborative dialogue between policymakers and citizens [22]. Open government is a multilateral process that involves elements of transparency, collaboration, and participatory governance [20]. Open government is the government's management and distribution of information and public services through various internet-based channels [23]. In general, open government can be understood as the governance of the relationship between the government and citizens based on digital information technology, which is carried out in a transparent, collaborative, and participatory manner.

Open government rests on the interactive relationship between the government and citizens. Good government-citizen relations must be based on two-way communication, which in open government is based on web-based dialogue [23]. Therefore, the open government runs on elements of government-citizen relations. Various experts identify these elements with different compositions but with interconnected ideas. Elements of open government include informing, engaging, and participating [24]. Elements of open government include transparency, openness, and engagement [23]. Elements of open government include transparency, participation, and collaboration [22]. Elements of open government include access to information, accountability, public participation, and data disclosure [20].

2.2. Surveillance State

The surveillance state is a digital governance concept that currently experiences significant development in practice in various countries. At first, the practice of surveillance or supervision of citizens was carried out for administrative purposes, then developed for anti-terrorism and geopolitics purposes, until now to protect the International and technological advances such as data analytics, machine learning, and artificial intelligence (AI) increasingly encourage the development of surveillance practice [25]. There are pros and cons to the current dynamics of the surveillance state development. On the one hand, surveillance practices can be an instrument for preventing instabilities and enforcing regulations [26]. On the other hand, surveillance practices create a relationship between the government as a watcher and citizens as watched, which can violate privacy [27].

The development of digital technology advances the practice of state surveillance into digital surveillance. The definition of digital surveillance is ”the act of real-time and retrospective viewing, processing and cataloging of online footprints against the will and/or knowledge of the actor(s) to whom such data belongs” [18]. Digital surveillance is the main instrument of the operation of a surveillance state that supervises citizens through digital technology. Digital surveillance generally consists of various domains ranging from data security, imagery, information & communication technology (ICT), geolocation, and biometrics [18]. Digital surveillance carried out on these citizens has various consequences on the lives of citizens [28]. In addition, various deviations from citizens' privacy and repression in the name of socio-political stability can also be the impact of digital surveillance.

Various countries implement digital surveillance at the policy level but with different schemes. Digital surveillance in China is implemented holistically, popularly known as the Great Firewall, which monitors activities in cyberspace through Deep Packet Inspection (DPI) and social mobility through AI. Russia has a legal instrument, the System for Operative Investigative Activities (SORM), which allows the government to monitor analog and electronic communications without notification. The United States also carries out digital surveillance through network surveillance, large-scale data collection and cataloging of real-time data for intelligence purposes. Meanwhile, European Union countries are trying to carry out digital surveillance balanced with transparency mechanisms related to data collection and use. The presence of the COVID-19 pandemic has become a momentum for strengthening the application of digital surveillance by various countries in the world. The COVID-19 pandemic has encouraged the incremental development of various surveillance technologies aimed at monitoring the spread of the pandemic and creating a pandemic surveillance state [19].

2.3. Public Safety vs. Citizen Privacy

The debate about surveillance state-based digital governance against the open government has developed along with technological advancements. On the one hand, the support for a surveillance state emphasizes the idea of public security. Supervision of citizens is considered necessary in order to detect various threats to public security. These threats include terrorism, counterintelligence, to the potential for political instability. Moreover, in its development, digital surveillance includes non-government surveillance carried out by private sector actors. Governments in various countries then try to build connectivity between government and non-government surveillance by

encouraging data collected on integrated non-government surveillance for government surveillance purposes [27]. Supporters of a surveillance emphasize that the state has the right to supervise citizens for public security and stability.

On the other hand, the open government block emphasizes the idea of citizens' right to privacy. This notion of privacy has evolved from personal to digital to global privacy. Privacy is freedom from various illegal intrusions (unauthorized intrusion) on personal information [18]. Digital privacy is freedom related to the formation of digital identity in which the dissemination of related information rests with the sovereignty of the individual owner [28]. Global-scale privacy is freedom from the illegal collection of information and surveillance of citizens outside the legal limits allowed [19]. Supporters of open government emphasize that there must be aspects of transparency, collaboration, and participation in digital governance between the government and citizens.

The dilemma between public security and citizens' privacy is getting sharper due to the presence of the COVID-19 pandemic [19]. In controlling the pandemic, strict tracking and supervision are carried out through facial recognition technology, surveillance cameras, AI, and mobile applications simultaneously suppress citizens' privacy [29]. Medical personnel groups encourage stricter surveillance practices to control the COVID-19 pandemic. Privacy and civil rights advocacy groups criticize the development of surveillance practices because they violate the fundamental rights of citizens. In this kind of situation, countries are required to balance public security and individual privacy [29].

3. Methods

The approach of this research is qualitative approach. The qualitative approach was chosen because it follows this study's purpose, namely, to describe the object of research in an elaborative and in-depth manner. The research object in question is the PeduliLindungi practice as an instrument of digital governance in Indonesia during the COVID-19 pandemic. The object of study will be analyzed using two theories, namely surveillance state, and open government. The particularity of each theory is still highlighted but with an analysis that is operationalized with an analytical matrix as follows:

The analysis in this study was carried out with a comparative theoretical model of the research object. This is done by analyzing aspects of (a) goals, (b) government-citizen relations, and (c) emphasis on PeduliLindungi. More specifically, in the aspect of objectives, it will be analyzed whether PeduliLindungi is more likely to achieve the goals

Table 1: Dichotomy of Surveillance State vs Open Government Elements.

Aspect	*Surveillance state*	*Open government*
Purpose	Country Stability	Digital Democracy
Government-Citizen Relationships	Watcher-Watched	Collaborative
Emphasis	Public Security	Privacy Rights Award

Source: Arranged by researchers (2022)

of state stability or digital democracy. In the aspect of government-citizen relations, it will be analyzed whether PeduliLindungi is more likely to be watcher-watched or collaborative. In the emphasis aspect, it will be analyzed whether PeduliLindungi is more likely to emphasize public security or respect for citizens' privacy. The analysis results of these three aspects will then be described to conclude whether PeduliLindungi is more likely to operate with a surveillance state or open government approach.

The data used are primary and secondary. Primary data is obtained through the direct use of various features and information in PeduliLindungi. Secondary data is obtained through related documents and reports. The data of these documents and reports include official reports of governmental bodies, non-governmental organizations, related books, journals, research reports, and news articles (from mainstream media). The analysis technique used is spiral data analysis from [30]. This spiral data analysis consists of 5 stages, namely: (1) data management and organization; (2) creation of new ideas; (3) description and classification of codification into themes; (4) build interpretations; (5) presentation of data in written form.

4. Results and Discussion

The assessment of the Surveillance State vs. Open Government elements was explored by examining the PeduliLindungi application features, terms, and conditions of application use, to the privacy policy implemented by the PeduliLindungi application. Furthermore, related previous studies and various secondary supporting sources such as scientific journals, books, and news articles are used. The words 'surveillance' and 'surveilans' are used interchangeably in this paper but still refer to the same concept.

4.1. State Stability or Digital Democracy?

Based on the Decree of the Minister of Communication and Information Number 171 of 2020 Concerning the Use of PeduliLindungi Applications in the Context of Implementing Health Surveillance for Handling Corona Virus Disease 2019 (COVID-19), the PeduliLindungi application is directed for several purposes including tracing; tracking, and quarantine enforcement [31]. Then it was refined through the Decree of the Minister of Communication and Information Number 253 of 2020 concerning Amendments to the Decree of the Minister of Communication and Information Number 171 of 2020 concerning the Use of the Peduli Lindungi Application for the Implementation of Health Surveillance for Handling Corona Virus Disease 2019 (COVID-19) [32]. This policy is an instrument for implementing the new-normal schemes.

In addition to tracing, tracking, and quarantine enforcement, there are several additional features in the form of e-certificates which include: 1) Rapid Test and/or Swab Test results; 2) Health Certificate; 3) a certificate of recovering from COVID-19; 2) vaccination certificate; 3) exit/entry permit; 4) agency assignment letter; and/or 7) other health certificates, there is also a global positioning system (GPS) monitoring, digital-based mobility tracking; to other defined features and/or collaboration with other platforms [33]. However, the regulation regarding the PeduliLindungi application was officially revoked as of 8 October 2021 through the Decree of the Minister of Communication and Information Number 459 of 2021 [34].

The Decree of the Minister of Communication and Information Number 253 of 2020 above does not explain the features contained in PeduliLindungi. Therefore, the researchers tried to explore the features of PeduliLindungi by installing the app and exploring the features [32]. Some of these features include: 1) scanning the required QR code when traveling to public places; users will be asked to scan the barcode provided at the entrance; 2) a zoning map that describes the user's location and the level of risk of COVID-19 transmission; 3) statistics containing information on the number of people infected with COVID-19 in a specific urban village, sub-district, city, or province; 4) vaccines, to see the status of COVID-19 vaccinations; 5) teledokter provide two services, namely independent medical examinations and consultations involving various types of existing health platforms; 6) downloadable COVID-19 vaccination certificates, so there is no need to print certificates; 7) user's travel history for the last two weeks. PeduliLindungi only records trips related to the system, for example, if the user checks in with the Scan QR code feature; 8) Electronic Health Card Alert (e-HAC)

belonging to the Ministry of Health, which is a user travel monitoring system during this pandemic; and other features that support government *surveilans* policies [35, 36].

From the description of the features above, this application relies on citizen participation to share citizen's mobility record while traveling so that contact history tracing with infected citizen can be carried out. Application users will also get a notification if they are in a crowd or in a red zone, which is an area indicated by a positive person infected with COVID-19 [37].

The word *'surveilans'* in the ministerial decree above in language *(Big Dictionary Indonesian)* can be interpreted as surveillance. Furthermore, the Oxford Dictionary defines 'surveillance' as the act of carefully watching a person suspected. Based on the purpose and meaning of the language, it can be concluded that the government uses the PeduliLindungi application as a tool to monitor the movement of citizens. The main goal of the mobility monitoring is aimed to ends the pandemic quickly and for state stability (health-political-social), including national economic recovery.

The app plays important roles in the state's efforts to monitor the movement of citizens who roam in public places and are at risk of transmitting the virus to other citizens. Throughout 2021-2022, PeduliLindungi has prevented 3,733,067 people with red status (incomplete vaccination) from entering public spaces and preventing 538,659 attempts of people infected with Covid-19 (black status) from traveling within the country or accessing public spaces [38]. So, it can be said that the massive use of PeduliLindungi has had a positive impact in carrying out *surveilans* policies that the government is pursuing to create the stability that the researcher meant above.

4.2. Watcher-Watched or Collaborative?

Watcher-Watched can be understood as a situation where the government can monitor/track the movement of the people but ignores their consent. Here the public is not given the space to disagree or reject the conditions put forward by the PeduliLindungi application, even ignoring the aspects of transparency and accountability. Watcher-Watched indicates that there is no feedback between the government and the public.

While collaboration can be interpreted as a condition of a mutually beneficial agreement between the two parties (the community and the government), it can not be said to be collaborative when the community is reluctant to download PeduliLindungi and agrees to provide data access to the application. Users of the PeduliLindungi application here have the freedom to agree or refuse to provide data access to the application. The government can access data from citizens only when citizens are willing to provide

access to their data. Collaborative also forbids the government from being coercive because citizens have complete control over their privacy rights. Until this research was conducted, there were more than 50 million downloads of PeduliLindungi on Google Play.

Based on data obtained by researchers from the application, especially in terms of use section, the application provides freedom for users to disagree with one, part, or all of the contents contained in the terms and conditions of use, and users are allowed to delete PeduliLindungi on electronic devices and/or not using PeduliLindungi. PeduliLindungi is not in charge from all responsibility for any losses the user receives in connection with the decision not to use PeduliLindungi [39].

When viewed on the pedulilindungi.id page, there are several policies for obtaining and collecting user data. The data are 1) Information on Registration Requirements which includes the National Identity Number (NIK), full name, date of birth, and mobile phone number; 2) Device Data Information which includes geographic location, time, and place. 3. Media and Photo files, including a photo gallery. Users can cancel the PeduliLindungi application permission at any time through the settings menu on the Smartphone [37]. PeduliLindungi will ask the user for access permission in advance to use the camera, gallery, and documents when the user downloads the vaccine certificate, uploading the document to complete the Electronic-Health Alert Card (e-HAC) based on the regulations set by the government. PeduliLindungi will not use and steal other information, data, or documents other than those authorized by the user [33].

The collaboration between the government and the community can also be seen in the development of PeduliLindungi. Based on data from Google Play, it can be seen that there are 1.01 million reviews from users where most people give reviews both praise and feedback/complaints about using the application. The government also responds to these inputs by providing the fastest solution and contacts the community can contact. In addition, based on the community's complaints, the government periodically improves the quality of PeduliLindungi. Apart from going through reviews on the application platform, the public can also provide reviews or input directly to the government, as was done by the Indonesian Internet Governance Forum (ID-IGF) by sending policy recommendation and input for the improvement of the PeduliLindungi application both in terms of application systems and governance. The recommendation was made, among other things, based on the number of complaints from users of the PeduliLindungi application submitted through various formal and informal forums [40, 41].

PeduliLindungi is not a tool/application that suddenly appears on people's devices and is used by the government to monitor people's movements. In this case, it can be concluded that PeduliLindungi is not coercive and still gives total freedom to users to refuse or grant access to their data, as evidenced by the existence of permissions (permission requests) that can be configured by PeduliLindungi users [37]. Furthermore, the collaboration between the government and the community will be mutually beneficial if, on the one hand, the government can fulfill its role in managing policies quickly and appropriately during the COVID-19 Pandemic through PeduliLindungi. However, on the other hand, the community can get the right to access public spaces because it is managed by PeduliLindungi [42].

4.3. Public Security or Privacy Rights Award?

Technological progress and economic development, raise serious concerns about violating personal privacy [43, 44]. Respect for privacy rights (personal privacy) is defined as "personal freedom," which is closely related to the issue of how people's data gets adequate protection so that there is no misuse of personal data [45]. Indonesia views privacy in personal data as part of human rights [46]. In the context of the PeduliLindungi application, it can be said to respect privacy rights when the government guarantees citizens' privacy rights despite tracking and tracing efforts to support surveillance policies in the era of the COVID-19 pandemic. When citizens uninstall the application, the government, through the PeduliLindungi application, has no right to track the movement of citizens [47].

The 1945 Constitution of the Republic of Indonesia Article 28 G paragraph (1) implicitly explains that the state has stated its commitment to protecting the community [48]. The following reads: "Everyone has the right to personal protection, family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something which is a human right." Furthermore, the protection of personal data and privacy rights is regulated in Law Number 19 of 2016 Concerning Information and Electronic Transactions (UU ITE) Article 26 paragraph (1) as follows: "... the use of any information through electronic media concerning a person's data must be carried out with the consent of the person concerned." [49]. Another principle contained in the privacy law in Indonesia is the Principle of Reliability, Security, and Responsibility, as stated in Article 15 and Article 16 of the UU ITE that electronic system operators are required to facilitate reliable and safe electronic systems and are responsible for the operation of the system and set implementation standards.

The National Cyber and Crypto Agency (BSSN) ensures that the COVID-19 contact tracing application (PeduliLindungi) has complied with personal data protection and security principles. The PeduliLindungi application has complied with the rules stipulated in Government Regulation Number 71 of 2019 Concerning the Implementation of Electronic Systems and Transactions article 14, paragraph 1, and article 15 [50]. PeduliLindungi has requested location and Bluetooth approval, then there is also personal data related to phone numbers and names, but their identities are anonymous. In terms of guaranteeing the rights of the owner of personal data, PeduliLindungi states that the data is stored in a database and is encrypted. Furthermore, the processing of personal data is also carried out by protecting the security of personal data from loss, misuse, unauthorized access, disclosure, and alteration or destruction of personal data. Regarding the point stipulating that data can be destroyed and deleted, it also applies to PeduliLindungi. In particular, personal data will be deleted from the application server for at least 5 (five) years since the application stops operating. BSSN also claims to have checked the security of an IT Security Assessment application, including the latest version of PeduliLindungi [51].

The government has regulated personal data protection with a particular scheme through PeduliLindungi. However, PeduliLindungi's security guarantee is still far from what is expected because it is still vulnerable to misuse of personal data. The vulnerability is because previously, there were no clear, comprehensive, and detailed rules regarding user protection and sanctions for misuse of the PeduliLindungi application [52], although recently, the Personal Data Protection Bill (PDP) has been approved for promulgation by the DPR together with the President [53]. The ratification of the bill also cannot guarantee the security of personal data because law enforcement will be weak. After all, it is under the president's authority. Their duties and authorities require them to be impartial or independent in examining and imposing sanctions on perpetrators [54, 55].

That is because public voices from various interest groups, including academics, continue to voice the immediate ratification of the Draft Law (RUU) on Personal Data Protection (PDP) into law so that it becomes legal certainty through various research and studies conducted [37, 52, 56, 57, 58], and other studies not listed here. Not only pressure, but the ratification of the Personal Data Protection Bill was also allegedly accelerated due to an issue that has recently gone viral, namely related to the hacking carried out by Bjorka hackers who claimed to have leaked personal data belonging to Indonesian citizens, including several public officials [59, 60].

Regardless of the dynamics of the policy after the ratification of the PDP Bill into law and the issue of hacking government and public personal data, the government continues to guarantee data protection and will continue to make improvements for the smooth use of PeduliLindungi. BSSN implements three safeguards for the PeduliLindungi system: application security, infrastructure security (including centralized data), and data security. BSSN also applies encryption to strengthen security when using the PeduliLindungi application. BSSN is also responsible for PeduliLindungi system security design and forensics if needed [61].

Even though the government has guaranteed the privacy and security of people's data, the government still needs always to be proactive and evaluative of the various possibilities. Indonesia has a lot to learn from Australia in terms of guaranteeing citizens' privacy rights and protecting people's personal data. Australia has comprehensive arrangements regulating personal data protection after COVID-19 ends, namely by providing criminal sanctions and fines for personal data breaches. Moreover, Australia also has a robust set of legal principles that protect the protection of personal data. Although Indonesia already has some personal data protection principles enshrined in national law, Indonesia needs to follow Australia to make sure that any entity that collects individual personal data can be based on personal data protection principles. The most important thing that must be applied in law in Indonesia in the context of implementing health surveillance applications to prevent COVID-19 is the imposition of sanctions to provide a deterrent effect on personal data breaches after the pandemic ends [62].

5. Conclusion

This study concludes that when viewed based on the features of the PeduliLindungi application, the terms, and conditions of use of the application, to the privacy policy applied by the PeduliLindungi application, the PeduliLindungi application is more oriented towards open government rather than a surveillance state. The conclusion was obtained from both aspects, namely the government-citizen relationship and the emphasis more inclined to open government, while only the purpose aspect was more inclined toward the surveillance state. To see a clear picture, the reader can see the results in table 2. which we have presented as follows.

In terms of purpose, PeduliLindungi emphasizes the country's stability because the purpose of PeduliLindungi is to control the movement of citizens to prevent COVID-19. Whereas in the aspect of government-citizen relations, it is more collaborative because

Table 2: Dichotomous Analysis Results of Surveillance State vs Open Government.

Aspect	*Surveillance state*	*Open government*
Purpose	**Country Stability (V)**	Digital Democracy
Government-Citizen Relationships	Watcher-Watched	**Collaborative (V)**
Emphasis	Public Security	**Privacy Rights Award (V)**

Source: Processed by researchers (2022)

it gives users the freedom to disagree with one, part, or all of the contents contained in the terms and conditions of use, users are given the freedom to delete PeduliLindungi and/or not use PeduliLindungi. Mutually beneficial collaboration can also be seen from the government's role in managing policies quickly and precisely during the COVID-19 Pandemic through PeduliLindungi. However, on the other hand, the community can get the right to carry out activities in public spaces. In addition, there is feedback between the people who provide input/complaints and the government, which response to these inputs/complaints. Finally, the emphasis of this application is more directed at respecting the right to privacy, as evidenced by the government's commitment to guarantee and maintain the privacy rights of citizens and the protection and security of people's data through a series of efforts made.

This study is a starting point in exploring the pandemic-based dynamics of digital governance in Indonesia. This study analyzes the tendency of PeduliLindungi, whether it leans more on open government or surveillance state principles. The analysis of this study focus on the features, terms & conditions and privacy policy of PeduliLindungi. Additionally, the study also analyzes the collaboration and feedback mechanism around PeduliLindungi. This study has limitations in analyzing the user/citizen experience in using PeduliLindungi and policy cycle over the development of PeduliLindungi. Therefore, future research to explore the citizen experience in using the PeduliLindungi is important to be conducted. More broadly, the research agenda to explore policy formulation, decision-making method, privacy-surveillance dilemma, and effectiveness evaluation of PeduliLindungi need to be conducted.

References

[1] Schwab K. The fourth industrial revolution [Internet]. World Economic Forum; 2017 [cited 2022 Sep 4]. Available from: https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

[2] Berdykulova GM, Sailov A, Kaliazhdarova S et al. The emerging digital economy: case of Kazakhstan. Procedia Soc Behav Sci. 2014;109:1287–1291. https://doi:10.1016/j.sbspro.2013.12.626

[3] Tierney T. The public space of social media: connected cultures of the network society. 1st Ed. London: Routledge; 2013.

[4] Clegg SR. The end of bureaucracy in Reinventing hierarchy and bureaucracy–from the bureau to network organizations. Diefenbach T, Todnem R, editor. Research in the Sociology of Organizations. Emerald Group Publishing Limited. 2012;35:59-84. https://doi.org/10.1108/S0733-558X(2012)0000035005

[5] Castells M. An introduction to the information age. City. 1997;2(7):6-16. DOI: 10.1080/13604819708900050

[6] Gascó-Hernández M. Open government: opportunities and challenges for public governance. Bolívar M, editor. Springer Science & Business Media. 2014; 4.

[7] Welchman L. Managing Chaos: Digital governance by design. New York, USA: Rosenfeld Media; 2015.

[8] World Bank. World Development Report 2009: Reshaping Economic Geography [Internet]. Washington DC: World Bank; 2009 [cited 2022 Sep 5]. Available from: https://openknowledge.worldbank.org/handle/10986/5991

[9] Kalvet T. Innovation: A factor explaining e-government success in Estonia. Electronic Government, An International Journal. 2012;9(2):142–157. https://doi:10.1504/EG.2012.046266

[10] Kitsing M. Success without strategy: E-Government development in Estonia. Policy and Internet. 2011;3(1):86–106. DOI:10.2202/1944-2866.1095.

[11] Sai AA, Boadi P. A bundled approach to explaining technological change: The case of e-Estonia. Eur J Bus Manag. 2017;9(30):1–17.

[12] Marx GT. Ethics for the New Surveillance. The Information Society. 1998;144(3):171-185. DOI: 10.1080/019722498128809

[13] Dirks E, Leibold, J. Genomic surveillance: Inside China's DNA Dragnet [Internet]. Barton: Australian Strategic Policy Institute; 2020 [cited 2022 Sep 6]. Available from: https://www.aspistrategist.org.au/genomic-surveillance-inside-chinas-dna-dragnet/

[14] Hoffman S. Engineering global consent: The Chinese Communist Party's data-driven power expansion [Internet]. Barton: Australian Strategic Policy Institute; 2019 [cited 2022 Sep 6]. Available from: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf

[15] WHO. Preventing and managing COVID-19 across long-term care services. WHO [Internet]. 2020 July 24 [cited 2022 Sep 6]. Available from:

https://www.who.int/publications/i/item/WHO-2019-nCoV-Policy_Brief-Long-term_Care-2020.1

[16] Olivia S, Gibson J, Nasrudin R. Indonesia in the time of Covid-19. Bulletin of Indonesian Economic Studies. 2020;56(2):143–174. doi: 10.1080/00074918.2020.1798581

[17] UNCTAD. China's structural transformation what can developing countries learn? New York: United Nations Publications; 2022.

[18] Ünver HA. Politics of Digital Surveillance, National Security and Privacy. Centre for Economics and Foreign Policy Studies [Internet]; 2018 [cited 2022 Sep 8]. Available from: https://www.jstor.org/stable/resrep17009#metadata_info_tab_contents

[19] Kampmark B. The pandemic surveillance state: an enduring legacy of COVID-19. J Glob Faul. 2020;7(1)59–70. doi: 10.13169/jglobfaul.7.1.0059

[20] Kopec A, Sheldrick, B. The adoption of open government by local governments in Canada: Obstacles and possibilities. Can J Urban Res. 2020;29(1)70–93.

[21] Shkabatur J. Transparency with(out) accountability: Open government in the United States. Yale Law Policy Rev. 2012;31(1):79–140.

[22] Evans AM, Camp A. Open Government Initiatives: Challenges of citizen participation. J Policy Anal Manag. 2013;32(1):172–185. doi: 10.1002/pam.21651

[23] Meer, Gelders D, Rotthier S. e-Democracy: Exploring the Current Stage of e-Government. J Info Policy. 2012;4(2014):489–506. https://doi.org/10.5325/jinfopoli.4.2014.0489

[24] Wanna J. Opening government: Transparency and engagement in the information age. In Opening Government. Wanna J, Vincent S, editor. Canberra, Australia: ANU Press; 2018. p. 3–24.

[25] Homan T, Pasquale A, Onoka K, Kiche I, Hiscox A, Mweresa C, et al. Profile: The Rusinga health and demographic surveillance system, Western Kenya. Int J Epidemiol. 2016;45(3): 718–727. doi: 10.1093/ije/dyw072

[26] Calvert G M, Higgins SA. Using surveillance data to promote occupational health and safety policies and practice at the state level: A Case Study. Am J Ind Med. 2010;53(2):188–193. doi: 10.1002/ajim.20707

[27] Richards NM. The dangers of surveillance. Harv Law Rev. 2013;126(7):1934–1965.

[28] O'Connor N, Lange A, Lange A. Privacy in the digital age. Great decisions [Internet]; 2015:17–28 [cited 2022 Sep 8]. Available from: http://www.jstor.org/stable/44214790

[29] Miyamoto I. Mass surveillance and individual privacy. Asia-Pacific Center for Security Studies [Internet]; 2020 [cited 2022 Sep 8]. Available from https://www.jstor.org/stable/resrep24871

[30] Creswell JW, Poth CN. Qualitative inquiry and research design (choosing among five approaches). 4^{th} ed. California: SAGE Publication, Inc; 2018.

[31] Decree of the Minister of Communication and Information Number 171 of 2020 concerning Determination of PeduliLindungi Applications in the Context of Implementing Health Surveillance for Handling Corona Virus Disease 2019 (COVID-19) (INA) https://jdih.kominfo.go.id/produk_hukum/view/id/735/t/keputusan+menteri+komunikasi+dan+informatika+nomor+171+tahun+2020

[32] Decree of the Minister of Communication and Information Number 253 of 2020 (INA) https://jdih.kominfo.go.id/produk_hukum/view/id/780/t/keputusan+menteri+komunikasi+dan+informatika+nomor+253+tahun+2020

[33] PeduliLindungi. PeduliLindungi Privacy Policy. PeduliLindungi [Internet]. 2022 Aug 8 [cited 2022 Sep 10]. Available from: https://www.pedulilindungi.id/kebijakan-privasi-data

[34] Decree of the Minister of Communication and Information Number 459 of 2021 (INA) https://jdih.kominfo.go.id/produk_hukum/view/id/816/t/keputusan+menteri+komunikasi+dan+informatika+nomor+459+tahun+2021

[35] Andarningtyas N. Exploring the features of the PeduliLindungi application. Antaranews [Internet]. 2021 Sep 4 [cited 2022 Sep 9]. Available from: https://www.antaranews.com/berita/2371566/mengulik-fitur-fitur-aplikasi-pedulilindungi

[36] PeduliLindungi. @PLindungi [Internet]. Twitter. What's new in PeduliLindungi January-March 2022; 2022 Mar 22. 2022 [cited 2022 Sep 9]. Available from: https://twitter.com/PLindungi/status/1506155866432573440

[37] Wijayanto H, Daryono D, Nasiroh S. Forensic analysis on the Peduli Lindungi application against leakage of personal data. J Info Comm Technol (TIKomSiN). 2021;9(2):11–18, 2021. doi: 10.30646/tikomsin.v9i2.572

[38] Rokom. PeduliLindungi Has Prevented Millions of Residents from Being Exposed to COVID-19. Sehat Negeriku, Ministry of Health of the Republic of Indonesia [Internet]. 2022 Apr 26 [cited 2022 Sep 10]. Available from: https://sehatnegeriku.kemkes.go.id/baca/rilis-media/20220415/3839664/pedulilindungi-telah-cegah-jutaan-warga-terpapar-covid-19/

[39] PeduliLindungi. PeduliLindungi Terms of Use. PeduliLindungi [Internet]. 2022 Aug 8 [cited 2022 Sep 10]. Available from: https://www.pedulilindungi.id/syarat-ketentuan

[40] Alfarizi MK, Wuragil Z. List of PeduliLindungi Application User Complaints and Recommendations for Improvement. Tempo.co. 2021 Sep 10 [cited 2022 Sep

10]. Available from: https://tekno.tempo.co/read/1504690/daftar-keluhan-pengguna-aplikasi-pedulilindungi-dan-rekomendasi-perbaikannya

[41] Mustopa A, Anna H, Pratama E, Hendini A, Risdiansyah D. Analysis of user reviews for the PeduliLindungi Application on Google Play Using the Support Vector Machine and Naive Bayes Algorithm Based on Particle Swarm Optimization. 2020 Fifth International Conference on Informatics and Computing (ICIC). 2020;2:1–7. doi: 10.1109/ICIC50835.2020.9288655

[42] Herdiana D. Peduli Lindungi Application: Community protection in accessing public facilities during the implementation of PPKM Policy. JIP: Jurnal Inovasi Penelitian. 2021;2(6):1685–1694. doi: 10.47492/jip.v2i6.959

[43] Liu J, Zhou S. Application research of data mining technology in personal privacy protection and material data analysis. Integrated Ferroelectrics. 2021;216(1):29–42. doi: 10.1080/10584587.2021.1911255

[44] Freeman EH. The telegraph and personal privacy: A historical and legal perspective. EDPACS (The EDP Audit, Control, and Security Newslette). 2012;46(6):9–20. doi: 10.1080/07366981.2012.750531

[45] Nugroho AA, Winanti A, Surahmad S. Personal data protection in Indonesia: Legal Perspective. International Journal of Multicultural and Multireligious Understanding. 2020;7(7):183–189. doi: 10.18415/ijmmu.v7i7.1773

[46] Rosadi S. Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. Brawijaya Law J. 2018;5(1):143–157. doi: 10.21776/ub.blj.2018.005.01.09

[47] Ministry of State Apparatus Empowerment and Bureaucratic Reform of the Republic of Indonesia. These are the Benefits of the PeduliLindungi Application that are Not Widely Known. Menpan [Internet]. 2021 Sep 10 [cited 2022 Sep 11]. Available from: https://menpan.go.id/site/berita-terkini/ini-manfaat-aplikasi-pedulilindungi-yang-belum-banyak-diketahui

[48] The 1945 Constitution of the Republic of Indonesia (INA) https://jdih.komisiyudisial.go.id/frontend/detail/3/4

[49] Law Number 19 of 2016 concerning Information and Electronic Transactions (INA) https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016

[50] Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (INA) https://peraturan.bpk.go.id/Home/Details/122030/pp-no-71-tahun-2019

[51] Gobel T, Suud Y. Ini Hasil Evaluasi BSSN terhadap Aplikasi Covid-19 PeduliLindungi. Cyberthreat.id [Internet]. 2020 Jun 29 [cited 2022 Sep 16]. Available from: https://cyberthreat.id/read/7325/Ini-Hasil%20Evaluasi-BSSN-terhadap-Aplikasi-Covid-19-PeduliLindungi

[52] Thaher I. Legal politics: Personal data protection on the PeduliLindungi application in Indonesia. Tambusai J Edu [Internet]. 2022;6(1):1065–1072 [cited 2022 Sep 17]. Available from: https://jptam.org/index.php/jptam/article/view/3068

[53] Yusuf. Minister of Communication and Informatics: PDP Bill Passed, Kominfo Oversees PSE Personal Data Governance. Directorate General of Informatics Applications, Ministry of Communication and Informatics of the Republic of Indonesia [Internet]. 2022 Sep 20 [cited 2022 Sep 24]. Available from: https://aptika.kominfo.go.id/2022/09/menkominfo-uu-pdp-disahkan-kominfo-awasi-tata-kelola-data-pribadi-pse/

[54] BBC News Indonesia. Personal Data Protection Law passed, but observers say its implementation has the potential to be a 'paper tiger'. BBC News Indonesia [Internet]. 2022 Sep 21 [cited 2022 Sep 25]. Available from: https://www.bbc.com/indonesia/articles/czq1e36l4jyo

[55] Jannah LM. UU Perlindungan Data Pribadi dan Tantangan Implementasinya. Fakultas Ilmu Administrasi Universitas Indonesia [Internet]. 2022 Sep 21 [cited 2022 Sep 25]. Available from: https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/

[56] Nurhidayati N, Sugiyah S, Yuliantari K. Personal data protection settings in the use of Pedulilindungi Application. Widya Cipta: Journal of Secretariat and Management. 2021;5(1):39–45. doi: 10.31294/widyacipta.v5i1.9447

[57] Djafar W. Personal data protection in Indonesia: Landscape, urgency, and need for renewal," public lecture "legal challenges in the era of big data analysis". Postgraduate Program, Faculty of Law, Gadjah Mada University. 2019;1(1):147–154.

[58] Dewi NK, Budiartha I, Subamia I. Responsibility of application health service providers Pedulilindungi Towards the Security of Consumer Personal Data. Journal of Legal Preferences. 2022;3(2):407–412. doi: 10.55637/jph.3.2.4952.407-412

[59] Dewi IR. Making Republic of Indonesia Excited, What Data Was Leaked by Bjorka Hackers? CNBC Indonesia [Internet]. 2022 Sep 14 [cited 2022 Sep 26]. Available from: https://www.cnbcindonesia.com/tech/20220914095826-37-371939/bikin-heboh-ri-data-apa-saja-yang-dibocorkan-hacker-bjorka

[60] Indriani RM. List of 7 'Secret' data leaked by Bjorka so far, shocking! Suara.com [Internet]. 2022 Sep 12 [cited 2022 Sep 26]. Available from:

https://www.suara.com/news/2022/09/12/110205/daftar-7-data-rahasia-yang-dibocorkan-oleh-bjorka-sejauh-ini-mengejutkan

[61] Agustini P. Pemerintah Jamin Sistem PeduliLindungi Aman. Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia [Internet]. 2021 Sep 9 [cited 2022 Sep 26]. Available from: https://aptika.kominfo.go.id/2021/09/pemerintah-jamin-sistem-pedulilindungi-aman/

[62] Olivia D, Rosadi S, Permata R. Protection of personal data in the implementation of the Pedulilindungi and Covidsafe Health Surveillance Applications in Indonesia and Australia. DATIN: Law Jurnal. 2020;1(2):1–15. doi: 10.36355/dlj.v1i2.453