Epidemic Intelligence Support System and Automated Processing of Personal Data

in South Korea

October 2021

정보인권연구소
Institute for Digital Rights

○ㄱ△름 인권재단사람

Epidemic Intelligence Support System and
Automated Processing of Personal Data
in South Korea
October 2021

Institute for Digital Rights
23, Dongnimmun-ro 8-gil,
Seodaemun-gu, Seoul,
Republic of Korea
03745

Written by Chang Yeo-kyung
Ttranslated by Ko Aram
Sponsored by Human Rights Foundation SARAM

Contact
https://idr.jinbo.net/category/english
idr.sec@gmail.com

Contents

1. Introduction

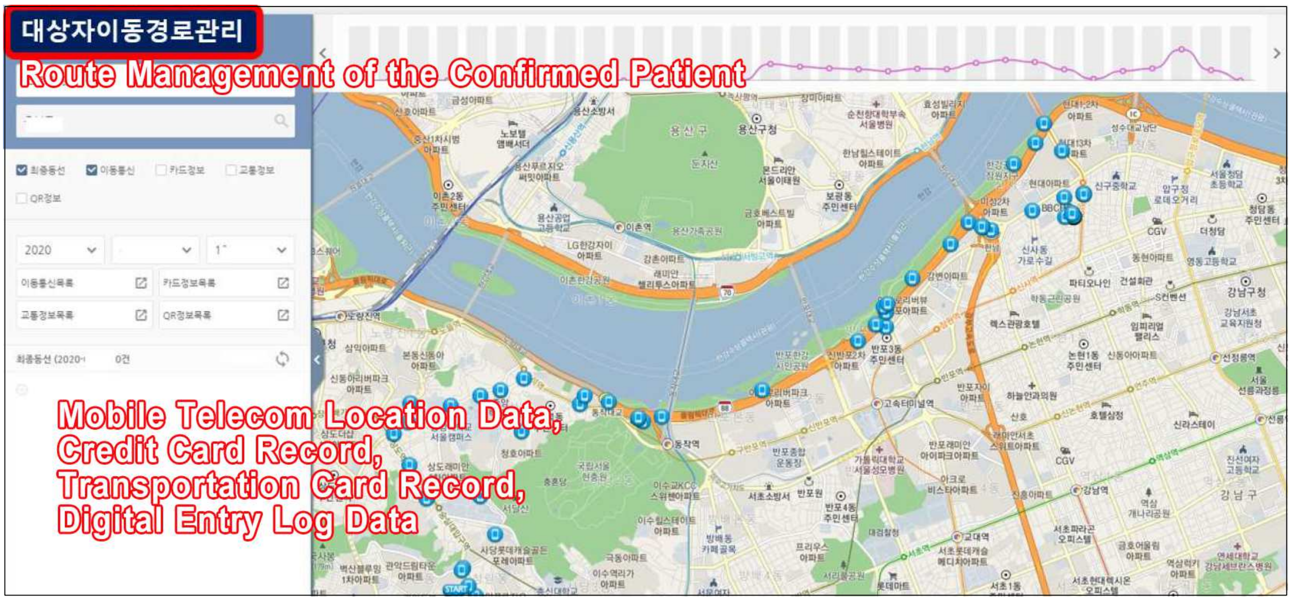
The Epidemic Intelligence Support System (EISS) has officially been in operation since March 26, 2020 to automate the epidemiological investigation procedure of the Coronavirus disease 2019 (COVID-19) after the pandemic. The EISS aims to automatically analyze the movement routes of confirmed patients by collecting and processing personal data from various public and private institutions.

The Ministry of Land, Infrastructure and Transport (MOLIT) developed EISS based on "Smart City Data Hub" technology—a real-time connection and sharing system for large-scale city data—and automated the process of requesting and receiving personal data from the Korea Centers for Disease Control and Prevention (KCDC), National Police Agency, Credit Finance Association, three telecommunication firms, and 22 credit card companies according to Article 76-2 of the Infectious Disease Control and Prevention Act (hereinafter the IDCPA). Afterward, the MOLIT transferred the system to the KCDC (currently the Korea Disease Control and Prevention Agency, KDCA) to use for epidemiological investigation of COVID-19.

The EISS is evaluated to have improved the speed and accuracy of personal data processing by automating the manual process of writing official documents and landline communication between 28 institutions. Also, it is appraised for its contribution to the reduced burden on epidemiological investigators so that they can swiftly respond to large-scale confirmed cases.

In 2021, development to strengthen the analysis and prediction functions of the EISS is in progress. The KDCA is developing a more advanced EISS that supports a sophisticated analysis and prediction of routes of confirmed cases using artificial intelligence (AI) which links resident registration information, immigration records, details of medical institution usage, and employee insurance information from the National Health Insurance Service. On the other hand, Bucheon City is pushing for an intelligent epidemiological system that automatically tracks confirmed patients and their contacts using facial recognition technology in images of street CCTVs and base station information. It also opens actual video datasets for the domestic AI industry after de-identification.

The Korean Government's Epidemic Intelligence Support System ▼


대상자이동경로관리
Route Management of the Confirmed Patient
☑ 최종동선 ☑ 이동동선 □ 카드정보 □ 교통정보
□ QR정보
2020
이동동선목록
카드정보목록
교통정보목록
QR정보목록
Mobile Telecom Location Data,
Credit Card Record,
Transportation Card Record,
Digital Entry Log Data
START

These institutions also announced plans to add targets for personal data collection and system connection to the IDCPA and its subordinate laws in order to provide a legal basis for the system under development. However, there is no provision of law planned to limit the analysis and prediction of sensitive personal data that becomes increasingly precise, the purpose and processing of the system, or ensure the rights of the data subjects.

The structure of the Personal Information Protection Act (PIPA) in Korea has not regulated “automated personal data processing” differently from general personal data processing, such as written documents. The problem is that with the development of digital communication technology, a plethora of more various types of personal data are being processed at a faster speed. As AI technology is applied to personal data processing methods in recent years, we are moving towards automated evaluation, analysis, prediction as well as decision-making. Compared to the methods in which personal data was processed manually or through paper documents, this change in personal data processing methods has a significant impact on the fundamental rights of data subjects, such as the right to the protection of personal data. Nevertheless, there is not enough discussion on the legal regulations.

The civil society in Korea has called the problematic human rights in such automated personal data processing “digital rights” and has demanded that they be guaranteed as fundamental rights protected by the Constitution. The social movement for digital rights has established, expanded, and developed subjects for protection, starting with the demand for rights to the protection of personal data to claiming rights not to be subjected to automated decision-making in the era of AI. The risk of infringement on fundamental rights is bound to increase as the means and methods of processing personal data are deployed in an automated manner (automated personal data processing), such as a database, rather than manually; as the influence of automatically processed personal data on the data subject for the purpose of evaluating, analyzing, and predicting individuals (profiling) becomes greater; and as more automated decisions that have legal or significant effects on individuals.

Chapter 2 outlines the progress of how Korean society developed by raising questions whenever the impact of the personal data processing methods on fundamental rights increased. Chapter 3 examines international norms related to automated personal data processing, such as profiling, and solely automated decision-making. Chapter 4 looks into problems with the EISS as a profiling system for sensitive data. Chapter 5 presents a legal regulation idea for the EISS to protect the rights of data subjects, and we concludes with Chapter 6.

2. Growing awareness of problems with automated personal data processing and fundamental rights

In the background of the protection of the right to personal information in Korean society as a system, civil society has constantly raised questions about the automation of personal information processing. As a result of related public interest litigations and legislative campaigns, the constitutional approval of the right to self-determination of personal information and the enactment of the PIPA have been achieved.
Before the 1997 presidential election, a human rights movement for digital rights against the “electronic resident card” emerged. The electronic resident card with a digital-communication type IC card was a change from the paper resident registration card. Citizens who remembered the anger they held towards the civilian surveillance incident of the military intelligence agency, Armed Forces Security Command, in 1990 were concerned about the advent of an electronic surveillance state when the Agency for National Security Planning, a national intelligence agency, led the electronic resident card project. The plan was to link the computer networks of police and passport issuance with the resident registration computer network of the Ministry of Home Affairs and other welfare-related computer networks, such as the medical insurance network and the national pension network, without any legal basis, while integrating 41 items in 7 fields (abstract/copy of resident registration, medical insurance, driver's license, national pension, registered seal, and fingerprint) in the electronic resident cards. Civil society organizations that formed a joint task force committee opposed this integration plan and demanded the guarantee of “privacy rights” based on the OECD guidelines.

This period was when international norms were established to protect data subjects from automated personal data processing. The OECD adopted privacy protection guidelines in 1980; the Council of Europe first opened the international convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) in 1981; the United Nations (UN) General Assembly adopted the “Guidelines for the Regulation of Computerized Personal Data Files” in 1990; the European Union (EU) established strong personal data protection guidelines by enacting the “Data Protection Directive” in 1995. It was a natural trend for Korean citizens to resist state surveillance and demand the right to the protection of personal data with their increased desire for democratization and human rights through the military dictatorships and civilian government. The civil society movement, in particular, paid attention to the risks of personal data processing methods based on digital communication and demanded the protection of personal data in accordance with international norms.

The then-presidential candidate, Kim Dae-jung, scrapped the electronic resident card after he was elected president since he was against it. However, the electronic government project that grafted digital communication technology into the administrative system continued. In 2003, voices against the personal data processing method of the government's National Education Information System (NEIS) grew. Civil society groups opposing the NEIS argued that the government managing the integrated database of metropolitan and provincial offices of education through a high-speed network (NEIS method) gravely violates the right to protection of personal data compared to each school storing information on students and parents on their school servers and principals processing them (CS method). At the time, the civil society movement asserted that people have “digital rights” that guarantee the right to protection of personal data in the information society. This was also when the government announced to introduce the concept of “fundamental informational rights” into the Constitution in the e-Korea Vision 2006 (the Third Master Plan for Informatization Promotion, 2002-2006) as demands for personal data protection and rights increased socially.

The National Human Rights Commission of Korea (NHRCK), which received complaints from teachers' organizations and civil society groups, recognized the human rights violations of NEIS in May 2003. At that time, Article 25 of the Elementary and Secondary Education Act stipulated that “The head of a school shall compile and manage the following data according to the standards determined by the Minister of Education and Human Resources Development after comprehensively observing and evaluating academic achievement, personality, etc. of students in order to use them for guiding and selecting students qualified to enroll in higher schools.” In addition, Article 23-2 of the Framework Act on Education stated that “The State and local governments shall devise necessary policies for electronic processing of administration of schools and educational organizations.” as a general regulation. The NHRCK believed that, despite these general regulations for the computerization of school administration and processing of personal data, there was a need for a specific legal basis to regulate NEIS. The Commission recommended to the Minister of Education and Human Resources Development to exclude areas such as health, with high risks of privacy infringement, from the NEIS method and use the CS method, which is the previous non-communication database method.

Afterward, in 2003, the government, teachers, parents, and civic groups agreed to enhance the NEIS system at the Committee for Educational Informatization established under the office of the Prime Minister. Moreover, Article 30-4 (Development and Operation of Educational Information System) of the Elementary and Secondary Education Act was newly established as a legal basis for NEIS on March 24, 2005. Currently, personal education data including personal health records is being processed by NEIS with this legal basis. The NEIS incident is considered to have dealt with the impacts on fundamental rights and its requirement for restrictions when the state collects, compiles, and manages sensitive personal data in a single database through a communication network compared to the manual method with non-communication.

Meanwhile, on May 26, 2005, the Constitutional Court approved “the right to self-determination of personal information” as a new independent fundamental right in a constitutional complaint filed by the civil society organizations against the national fingerprinting system (Case 99Hun-Ma513 etc). In particular, the Court stated that the right to self-determination of personal information is “ultimately the minimum constitutional guarantee necessary to protect individual freedom of decision and furthermore, to block the possibility that the foundation of the free democratic system will be totally damaged by protecting your personal information against the risks inherent in the new information environment, where it is possible for all organizations to use the personal information held by one institution at the same time as information exchange between various institutions becomes easier through the automation of information processing and the combination of information files.”
Nevertheless, in this case, the Constitutional Court considered that the general regulation of the former Act on Protection of Personal Information in Public Institutions and police-related laws were sufficient for the police to computerize and use fingerprint data of all citizens. Also, the Court decided that the NEIS can process personal data based on the general regulation of aforementioned former Act on Protection of Personal Information in Public Institutions and the Elementary and Secondary Education Act, and dismissed the constitutional petition for the NEIS case on July 21, 2005 (Case 2003Hun-Ma282). The court’s opinion considered that it is constitutional to process sensitive personal data at large scale on the national automated computerization systems, based on general regulations, such as “public institutions may retain personal information files where it is necessary for a public institution’s performance of their duties under its jurisdiction”(Article 5 of the former Act on Protection of Personal Information in Public Institutions).

However, Judge Kwon Seong opposed to setting the basis for processing personal data regarding sensitive academic background in the general regulations that significantly lacked specificity in the purpose of information collection and processing. Judge Kwon Seong disagreed with the court’s opinion, saying, “The electronic information processing system that builds and manages an integrated database like NEIS by interconnecting it has a very high degree of restriction on the right to self-determination of personal information in terms of information processing method.” He stated, “In order to justify this type of personal data processing, the scope of the information process must be minimized, and the purpose of processing personal data must be clearly specified at the collection stage, and the information must be stored, used, and relayed only for that specific purpose." He continued to emphasize, "Stronger protection is required the more personal data is held and processed in the form of computer files rather than handwritten documents and the more personal data is held and managed in one integrated system than stored after distribution. It is easier to access, combine, and use personal data in this manner. Even sporadic personal data that does not require much protection may be organically combined with other personal data through an automatic search system, so that an individual's overall and partial individuality may be under the supervision and control of state power."

This opposing opinion saw that the state's method of integrating sensitive information into a single database through digital networks requires stronger protection than processing through manual distribution. Furthermore, the contrary view believed the legal grounds requiring such restrictions on fundamental rights should specifically stipulate the purpose, scope, and limitation of processing and not be based on general regulations.

After the NEIS controversy, the social demand for the enactment of a framework act on personal data protection increased. A civil society bill (representative bill by Roh Hoe-chan), the ruling Uri Party's bill (representative bill by Lee Eun-young), and the opposition Grand National Party's bill (representative bill by Lee Hye-hoon) were proposed consecutively during the 17th National Assembly. Consequently, the PIPA was enacted and enforced on March 11, 2011 with the Lee Myung-bak administration and the 18th National Assembly.

Since the enactment of the PIPA much of the problems raised by judges Kwon Sung are currently regulated by the Principles for Protecting Personal Information (Article 3 of PIPA), such as the principle of purpose limitation and the principle of data minimization. However, the PIPA adopts an approach that regulates collectively regardless of the digital or handwritten form, or the automatic or manual processing of personal data. Therefore, the PIPA does not specifically regulate the so-called "profiling" in which different personal data is organically combined through automatic processing and affects the overall and partial individuality of citizens. The PIPA neither defines the concept and risks of automated personal data processing, such as profiling, nor stipulates restrictions or protection that are distinct from general personal data processing.

Recently, as services and products using AI are rapidly increasing in each field of society, the problem of solely automated decision making using personal data of data subjects is increasing. Civil society organizations have filed an information disclosure lawsuit demanding transparency in the AI recruitment process of public institutions, and riders are demanding workers' rights to solely automated allocation and rating of delivery platforms. However, PIPA does not have a provision to protect the rights of data subjects from solely automated decision making.

In Europe, on the other hand, efforts have been made to define and regulate automated personal data processing, such as profiling. In the following, the concept of automated personal data processing and regulations governing it will be examined, focusing on the European legal system for personal data protection.

3. European norms for automated personal data processing and profiling

A. Concept of profiling

In Europe, legal and institutional rules have been sought for automated personal data processing and decision based solely on automated processing, and the concept of “profiling” lies at the core of these rules.

“Profiling”means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Broadly speaking, profiling is gathering information about an individual or group of individuals and analyzing their characteristics or behavior patterns in order to place them into a certain category or group, and/or to make predictions or assessments about their ability to perform a task, interests, or likely behavior.

In other words, profiling is consists of three elements: (1) automated form of processing; (2) carried out on personal data; and (3) the objective of profiling which must be to evaluate personal aspects about a natural person. A simple classification of individual data that does not include evaluation, analysis, or prediction does not constitute profiling. Moreover, profiling is a procedure that may involve a series of statistical inferences. This includes analyzing an individual using data from various sources to infer something about that person based on the qualities of individuals who appear statistically similar.

Profiling is a form of automated personal data processing and usually includes personal data processing. At this time, only partial elements of the personal data may be included, not the complete form. Although profiling is commonly related to automated decision-making, it may not lead to a solely automated decision-making. For example, when a firm generates profiles for certain consumers, it categorizes (carrying titles such as “Rural and Barely Making It,” “Ethnic Second-City Strugglers,” and “Tough Start: Young Single Parents”) or “scores” them, focusing on consumers’ financial vulnerability, rather than only use the existing personal data as their basis. Meanwhile, imposing speeding fines purely based on the evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling. However, a decision may be based on profiling if the driving habits of an individual were monitored over time, and the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations. A bank may consider the credit score of the borrower, with additional meaningful intervention carried out by humans before any decision is applied to an individual before granting a mortgage. In this case, decisions include profiling, but are not solely automated.

The EU’s “Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679” explains the rules of profiling. The guildelines point out that while profiling has the benefits of increased efficiencies and resource saving, the process can be opaque in the sense that individuals might not know that they are being profiled or understand what is involved. Furthermore, profiling can lock a person into a specific category and restrict them to their suggested preferences. It can also perpetuate existing stereotypes and social segregation. This can lead to erroneous predictions, unfair refusal to provide services and goods, or unfair discrimination.

As such, automated personal data processing, including profiling, that leads to decision-making has a greater impact on data subjects and higher risks than general personal data processing. In 1995, the EU stipulated the concept of “automated individual decisions”in Article 15 of the “Data Protection Directive” to regulate these issues. In 2010, the Council of Europe tried to define “profiling” more specifically and regulate automated personal data processing in “The protection of individuals with regard to automatic processing of personal data in the context of profiling". This recommendation suggests in the process of profiling:

- complying with the principles of personal data processing such as lawfulness;
- ensuring data quality such as accuracy;
- abiding by processing requirements for sensitive data;
- providing information to data subjects;
- guaranteeing the rights of data subjects;
- having exceptions and restrictions;
- assuring remedies;
- providing data security;
- and supervisory authority regulations.

Legal regualtions over profiling of the EU and the Council of Europe was established as a unified norm in the General Data Protection Regulation (GDPR). The GDPR is the basis for general profiling and solely automated decision-making and regulates profiling separately. In March 2021, for example, the Amsterdam District Court in the Netherlands separately ruled that the vehicle-sharing platforms, Ola and Uber, should disclose the personal data requested by workers. The applicable legal provisions differed depending on whether it was general profiling or profiling based on solely automated decision-making. Each of the processing principles will be examined in the following part.

B. Principles of general profiling process

General profiling is a type of personal data processing method and is subject to all general principles of personal data processing required by the GDPR. Although profiling processes the personal data of the data subject directly, sometimes it uses evaluation, analysis, and prediction such as scoring or classification of data subjects. Hence, Article 4(4) defines profiling separately to differentiate it from the existing personal data processing.

When a controller processes personal data, they must comply with the principle of lawfulness, fairness, and transparency in the GDPR (Article 5(1)(a)). The reason the transparency of processing is emphasized here is because profiling process is normally invisible to the data subject. It works by generating "new" personal data that has not been provided directly by the data subjects themselves. In other words, profiling operates by creating derived or inferred data about individuals. Therefore, individuals have different levels of comprehension and it might be difficult for them to understand the complex techniques of profiling and automated decision-making processes. Hence, data subjects must be provided with concise, transparent, intelligible and easily accessible information about the profiling processes. Moreover, fairness must be ensured since profiling may be unfair and discriminating.

In addition, the GDPR provided principles for compliance regarding additional processing and purpose limitation (Article 5(1)(b)), data minimization (Article 5(1)(c)), accuracy (Article 5(1)(d)), and storage limitation (Article 5(1)(e)). In particular, it is necessary to pay attention to the principle of accuracy in the profiling process. If the data used in the automated decision-making or profiling process is outdated or inaccurate, the decision or the profiling made based on that data will be erroneous. Inaccurate data can lead to inappropriate predictions or statements about an individual's health, credit or insurance risk. Even if the raw data was accurately recorded, the dataset may not be fully representative or the analytics may have hidden biases. As a result, the controller must introduce measures to continuously check the data reused or obtained indirectly is accurate and up to date. The controller should also provide the data subject with clear information about the processed personal data to correct any inaccuracies and improve the quality of the data. In addition, machine-learning algorithms are also often designed to process and correlate large volumes of information to generate comprehensive and intimate profiles of individuals, and there will be more data that this algorithm can learn from. Accordingly, the controller must comply with the principle of data minimization and ensure that the personal data is stored for no longer than a period necessary and proportionate for the purpose of processing personal data.

On the other hand, as with general personal data processing under the GDPR, profiling must also satisfy the lawful bases for its processing, which include: (a) the consent of the data subject; (b) the performance of a contract; (c) the compliance with a legal obligation; (d) the protection of vital interests; (e) the performance of a task in the public interest or the exercise of official authority; and (f) the legitimate interests by the controller or a third party (Article 6(1)).

In particular, if sensitive data, such as data concerning health, is involved in profiling, it can be processed only in special circumstances. These circumstances are if: (a) the data subject has given explicit consent; (b) processing is in the field of employment, social security or social protection laws, (c) processing is necessary for the vital interests in situations in where the data subject cannot give consent; (d) processing is carried out in the course of legitimate activities with political, philosophical, religious or trade-union aim; (e) the data subject manifestly made public personal data; (f) processing is necessary for legal claims or court actions; (g) processing is necessary for reasons of substantial public interest on the basis of law; (h) processing is necessary for the provision of health or social care or treatment, or the management of health or social care systems and services based on law; (i) processing is necessary for reasons of public interest in the area of public health based on law; and (j) pseudonymizing for public archiving, scientific or historical research purposes, and statistical purposes based on law (Article 9(2)). The GDPR also stipulates the necessary requirements for each law. In the case of (b), it must be a law "providing for appropriate safeguards for the fundamental rights and the interests of the data subject."For (g), the law should be"proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." The law in (h) must stipulate the duty of professional secrecy, and in case (i), the law should "provide for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy." For (j), the law "shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." Meanwhile, Article 36(5) of the GDPR stipulates "Member State law may require controllers to consult with, and obtain prior authorization from, the supervisory authority in relation to processing ... in the public interest, including processing in relation to social protection and public health."

Furthermore, the data subject has the right to be informed of their profiling (Articles 13 and 14), access their profiling (Article 15), and rectify, erase, or restrict processing (Articles 16 through 18). In this case, the data subject is generally informed about the consequences of profiling, such as the existence and the related decision-making, and has the right to object it in specific circumstances (Preamble 60). The right to access profiling and rectify, erase, and restrict processing apply to all, including the personal data input used to create the profile, the profile itself, and the output data such as the segment or score granted to the data subject. The right to object (Article 21) can be exercised when the profiling is necessary for performance of a task in the public interest (Article 6(1)(e)) or legitimate interests by the controller or a third party (Article 6(1)(f)). In the case of a task for public interest, personal data may have to be erased at the request of the data subject if there is no compelling legitimate grounds that override the objection of the data subject. To have compelling legitimate grounds, the controller must prove that profiling is important for a specific purpose of public interest, is limited to the minimum necessary to meet the purpose, and that a balancing exercise is carried out.

As such, the GDPR regulates profiling along with general personal data processing, but also has stricter regulations due to the risks of profiling. Profiling used in solely automated decision-making is prohibited in principle, and even if profiling does not lead to solely automated decision-making, data protection impact assessment is mandatory if any systematic and extensive evaluation of personal aspects is carried out and the decision-making has any legal or significant impact (Articles 35 and Preamble 91). The controller must take protective measures to address the risks revealed as a result of the impact assessment. The protection measures include notifying the data subject of the existence of profiling, specific and meaningful information on the related logic, the significance of processing, and the envisaged consequences of it. Ensuring the right of the data subject to oppose the decision and express their points of view is also part of it. Consultation with the supervisory authority of data protection is required if the risks are still high.

C. Profiling of solely automated decision-making

With the emergence of new technologies such as AI, the GDPR established a system to protect data subjects believing automated individual decision-making, including profiling, poses a significant risk to the fundamental rights of data subjects. The GDPR stipulates provisions for “automated individual decision-making, including profiling” in Article 22 and has general prohibition when 1) a decision that has legal effects or a similar significant affects data subject 2) is processed by automatically and 3) is solely based on automated processes. The prohibition does not seek proactive objection from the data subject.

Among these, the case of “similarly significantly affects” means that even if there is no change in legal rights or obligations, it may significantly affect an individual's circumstances, behaviors or choices, such as “automatic refusal of an online credit application” or “e-recruiting practices without any human intervention,” or has a prolonged or permanent impact on data subjects, or where individuals are excluded or discriminated (Preamble 71). For example, a credit card company may have lowered the card limit based on an analysis of other customers in the same region who shopped at the same store, not the actual consumer's own repayment history. Depriving a consumer of opportunities due to the actions of others can be recognized as a decision that significantly affects data subjects.

On the other hand, not to be solely automated, human oversight of decision-making must be made in a meaningful manner and not just a gesture, and a person with the authority and competence to change decision-making must intervene, and all relevant data must be reviewed by a person at the analysis stage.

However, solely automated decision-making is exceptionally permitted when it is necessary for the performance of or entering into a contract, authorized by law, and is based on the explicit consent of the data subject. In particular, to conduct solely automated decision-making for reasons of contract signing and implementation, profiling must be a necessary process for achieving the purpose. If there are privacy-intrusive method to achieve the same goal, it does not apply. A solely automated decision-making based on sensitive data can be made only if there is explicit consent of the data subject, or for significant public interest reasons based on law and measures for data subject protection exist.

In all cases where solely automated decisions are made as an exception, protective measures must be made to safeguard the rights, freedoms, and legitimate interests of the data subject. The protection measures at this time are to inform the data subject beforehand about the existence of profiling and solely automated decisions, the sufficient and significant information about the relevant logic, and the significance and envisaged consequences of processing. These measures should also guarantee the data subject with the rights to obtain human intervention, express their points of view, obtain an explanation of the decision, and challenge the decision. Moreover, the controller should check for bias in the processed dataset and develop measures to address this problem. Another useful measure would be to audit algorithms, review the accuracy and relevance of automated decision-making periodically, and feed back the outcomes into its system design.

D. Comparison with the norms of Korean PIPA

The PIPA does not have a separate protection standard to limit automated analysis, evaluation, and prediction, such as profiling, and protect data subjects from such processing. This restricts the Personal Information Protection Commission (PIPC) in their judgement on automated personal data processing or decision-making such as profiling.

On May 25, 2020, the PIPC decided that the “vehicle operation information verification system” of MOLIT could automatically share and process vehicle recognition data identified by the vehicles targeted by crackdown and CCTV images between local governments and the central government and make decisions, such as administrative disposition (Resolution

2020-10-178). This decision was considered to satisfy the lawfulness of Article 18(2)2 of the PIPA, as there is a general provision for requesting and submitting data “when necessary” for relevant tasks, such as Article 72(2) of the Motor Vehicle Management Act. However, the PIPC did not examine the legal basis for automatically analyzing personal data or automatically making decisions for unmanned crackdowns or cancellation of registration. This is because the PIPA does not stipulate the relevant details.

However, as discussed in Chapter 2, processing personal data through automated methods, such as profiling, and going further to making automated decisions will increase the risk of infringement on fundamental rights compared to conventional personal data processing forms, such as manual methods. In Europe, personal data protection laws have also shown a trend of strengthening protection norms from automated personal data processing, such as profiling, to solely automated decision-making. In particular, it will be possible to protect the rights of data subjects only when profiling is clearly defined since it is distinct from existing personal data processing. This is especially so given that profiling generates information that partially contains personal data or combines information from various sources.

Therefore, it is necessary to legally define and regulate the concept of profiling in the legal system. If general profiling is included as one of the automated forms of personal data processing, it may be governed according to general personal data processing regulations. In the case of profiling, in particular, it is necessary to ensure fair and transparent processing, limit purposes, restrict data for processing to its minimum, ensure accuracy, and set storage limitation. The current PIPA stipulates not only the principles for protecting personal information (Article 3), but also restrictions on the collection and use of personal information (Article 15), the limitation to the collection (Article 16), and the obligation of destruction (Article 21). Hence, it seems possible to regulate profiling according to this Act. Yet, the principle of ensuring accuracy (Article 3(3)) of the PIPA is restricted to a declarative application, and the details about prior information to ensure transparency fall very short of the GDPR. It seems the regulations require supplementation. In particular, it is necessary to prepare regulations to ensure that the data subjects receive prior information of the profiling, such as the existence of profiling and related consequences such as decisions, and explain their rights to exercise their objections in certain circumstances.

Above all, profiling that lead to evaluation, analysis, and prediction of an individual based on sensitive data, such as health related data, in itself has a significant impact on the fundamental rights of the data subject. Consequently, the provisions of laws that require or permit this must ensure that there are significant reasons of public interest and stipulate appropriate and specific measures to protect the fundamental rights and legitimate interests of the data subject.

Additionally, the data subjects should be guaranteed their the rights to access, rectify, erase, or suspend processing not only for the input data but also for the output data of profiling. Currently, the data protection impact assessment is also conducted at the discretion of the personal information controller as a formality. It is necessary to strengthen the accountability of the personal information controller by strengthening this practice as a practical norm.

In principle, processing leading to solely automated decision-making based on profiling should be prohibited. In March 2021, as the PIPC pushed to amend the PIPA, the PIPC newly established provisions on the “right on the automated decisions” in the legislative notice, allowing data subjects to object, challenge, and demand explanations for solely automated decisions (Article 37-2 of the bill). However, the legislative notice basically enables solely automated decision-making and is limited in that it guarantees the right to object only in certain circumstances of processing when personal information is collected from data subjects or third parties under Article 15 of the PIPA. There is no protection for solely automated decision-making based on profiling that generates information derived or inferred from the data subject by combining information from various sources. The data subject is not guaranteed the right to receive advanced information of the profiling, and the logic and consequences of automated decisions. The data subject is not even ensured the right express their opinion or demand human intervention.

In its opinion on the legislative notice, the NHRCK pointed out that in principle the data subject has the right not to be subject to a solely automated decision. The NHRCK considered it desirable to only allow automated decision-making to an exceptionally reasonable and legitimate extent rather than applying it generally to the data subject. It was also pointed out that stricter conditions such as "when the law permits for serious public interest purposes" and "clear consent of the data subject" need to be defined when processing sensitive information generated by automated decision-making.

The evident systematic limitations of the PIPA compared to the GDPR are leading to a gap in regulation on profiling sensitive information processed in the EISS and the current pandemic situation.

4. Automated personal data processing and profiling of EISS

A. Overview of EISS

According to the National Assembly audit data, the number of personal data collected by the EISS for COVID-19 was 10,073 as of October 2020 and continues to increase. The retention period is de facto semi-permanent. The KDCA announced that it would destroy all personal data collected through the EISS at the end of the long-term epidemiological investigation of COVID-19. However, KDCA's stance is that it may not destroy the personal data collected so far if COVID-19 does not come to a complete end and a few cases continue to exist.

The EISS users are epidemiological investigators of KDCA and local governments. They receive information of confirmed cases on locations, credit cards, and transportation cards from mobile carriers and credit card companies to analyze and use for epidemiological investigation. System functions related to the provision of personal data of confirmed cases are also accessible to officials from the National Police Agency, mobile carriers, Credit Finance Association, and credit card companies. They also receive QR-code information of the digital customer entry logs from Korea Social Security Information Service, one of the government commissioned public institutions.

The location information of the mobile carriers processed at this time is the names, mobile phone numbers, dates, times, latitudes, and longitudes of the confirmed persons. The data from the credit and transportation cards of the credit card companies is the names, transaction dates and times, names and numbers of the affiliated stores, and transaction amounts. The information of the digital customer entry logs includes the names, mobile phone numbers, facility information, and time of visits.

The epidemiological investigators register the confirmed cases in the system and request their personal data through the process of the EISS. The mobile carriers and credit card companies that receive the requests upload the related data to the system, and the data is converted and stored according to the Smart City Data Hub model which is the basis for EISS operations.

Since base stations are used for the location information, there are slight discrepancies from the actual movement of the confirmed patient. The errors can be from several tens of meters in the downtown area to several kilometers in the suburbs, and many actual data errors exist. To solve this problem, the actual movement of the confirmed person is estimated by applying machine learning that includes data purification based on the threshold of the confirmed person's travel speed (e.g. a person cannot move faster than a car, train, or other means of transportation) and various algorithms of interpolation, clustering, and classification. There were cases, although very few, where the information provided by the system did not match the statement of the confirmed case. In June 2020, Daejeon City filed a criminal complaint for cheating against a confirmed person whose location information indicated by the GPS location data did not coincide with his/her statement. However, the prosecution investigated the actual case and dropped the charges against the person.

With the start of 2021, the KDCA and Bucheon City of Gyeonggi-do are developing enhanced analysis and prediction functions of EISS, respectively.

First, the KDCA will develop an “in-depth” EISS by November 2021 that adds personal data from multiple ministries to analyze the movement of confirmed patients more precisely—resident registration information from the Ministry of Interior and Safety; immigration records from the Ministry of Justice; history of medical institution usage from the Health Insurance Review and Assessment Service; and employee insurance information from NHIS. The new system will use AI to support analysis and prediction of the date of disease development, source of infection, location of local infection risk, etc.

The functions of the in-depth EISS for more precise data on confirmed cases include: automatic verification, input and inquiry of data on domestic confirmed cases by linking information of confirmed patients, resident registration, and employee insurance; automatic verification, input and inquiry of immigration and treatment information; and risk-level check such as medical institution usage history. In addition, it plans to provide close analysis of infection information of confirmed cases including cause of infection and risk of infection by date; risk analysis of regional infection; and mass infection management services such as cluster management of confirmed patients and their contacts.

The in-depth EISS aims to minimize human intervention by increasing the level of automated process for linked data input compared to the current system. The plan is to connect the closed public administration network—information has been provided manually to process official documents—to an external cloud network in the private sector. This change in personal data processing method can be seen as increasing the risk in terms of the impact on the fundamental rights of data subjects. The in-depth EISS will expand beyond the current COVID-19 target system to general infectious diseases (2022), and continue to operate by converging with the existing KCDA epidemiological investigation system (2023).

On the other hand, Bucheon City is developing an “intelligent epidemiological system.” The main focus of the system is to analyze the movement of confirmed patients and close contacts through facial recognition in the footage of CCTVs that are integrated and controlled by the city, and identify the contact's identity through location information from nearby base stations. The intelligent epidemiological system plans to go national connected to the existing EISS. It also includes plans to de-identify actual dataset such as facial recognition data of confirmed patients and contacts and open them for the AI industry. Through this system, Bucheon City expects to solve problems such as the excessive procedure and time required for video data acquisition in current epidemiological investigations; lack of accuracy and time in the tasks of epidemiological investigators; inadequate system to swiftly track suspected cases in unspecified masses, assemblies, and high-density spaces; reduced health-worker operation efficiency; absence of contact-tracking service for individuals; and personal data concerns.

The functional implementation of the intelligent epidemiological system is as follows. First, it recognizes the face of the confirmed patient based on the video data by the quarantine authorities, such as public health centers, and tracks the movement route in the street CCTV image for analysis. It also analyzes close contacts, checking their proximity and whether they are wearing mask. Next, it further scrutinizes the movement of the close contacts, collects location data from nearby base stations, and automatically verifies their identities. The intelligent epidemiological system analyzes areas at risk of infectious diseases based on big data such as regional population density, fixed and floating population, and temporal and spatial information related to environment and geography, and attempts to predict the spread of infectious diseases. In addition to providing information on infection spread as an API service after de-identification so that individuals can compare with the movement records stored in their smartphones, it provides a contact tracing function that is available to the quarantine authorities in case of confirmation.

In the short term, the project aims to establish an intelligent epidemiological system that tracks people using artificial intelligence and promote data sharing such as card and location information of confirmed cases and their contacts in connection with the existing EISS. In the long term, the project will build a dataset for AI learning based on actual CCTV image data, which will be available after de-identification processing to expand the AI tracking market. The system will be upgraded in the future to apply to tracking and managing missing children and criminals.

In conclusion, both current and future systems related to epidemiological investigation aim to link and combine personal data from various sources to automate analysis and prediction of the movements of confirmed cases and their contacts who are the data subjects. The current EISS automatically analyzes the movements of confirmed patients by the hour based on multiple sources of personal data, and performs automatic analysis of infection networks and areas at risk of infection. When the subject of analysis involves an individual, such as contacts, this is an automated prediction of an individual. Moreover, the in-depth EISS under development by the KCDA will analyze the movements of confirmed cases of infectious diseases in more detail based on more sources and perform a more automated analysis and predictions using AI functions. If an individual is involved in the source or area at risk of infection performed by this system, this can also be considered as an automated prediction of the individual. The intelligent epidemiological system Bucheon City is developing aims to automate analysis of the movements of confirmed patients and their contacts through processing of unspecified number of facial recognition data in public places and automatically predict the risk of contact and spread of infectious diseases.

B. Personal data processing of EISS

From the time of the launch in March 2020, the EISS received information on location, credit card, and transportation card as data to identify the movement routes of confirmed patients (hereinafter referred to as "route information"), QR-code based entry logs were added to this list in July of the same year. The legal basis for processing these route information is Article 76-2 (Request for Provision of Information and Verification of Information) of the IDCPA, Article 32-2 (Information Requestable to be Provided) of the Enforcement Decree of the IDCPA, and Article 47-2 (Targets of Information Provision to Prevent Spread of Infectious Diseases) of the Enforcement Regulation. The provisions of the Act were newly amended on July 6, 2015, allowing quarantine authorities to request and receive personal data for epidemiological investigations prior to the COVID-19 crisis, and were not specifically governing automated personal data processing through the personal data processing system.

The basis for the lawfulness of processing each route information performed by the EISS is as follows: Article 76-2(2) of the IDCPA for location information, Article 32-2(1) of the Enforcement Decree of the IDCPA for credit card information, and Article 32-2(2) of the Enforcement Decree for transportation card information. However, in the case of information for QR-code based entry logs, the IDCPA stipulates the obligation to prepare a list of visitors only for places or facilities at risk of spreading infectious diseases (Article 49(1)2-2) with the amendment of the IDCPA in August 2020. The provision to third parties such as quarantine authorities is based on the consent of the data subject.

Meanwhile, the systems currently under development plan to establish additional legal grounds through revision of enforcement decrees. The in-depth EISS of the KDCA plans to revise Article 22-3(3) of the IDCPA Enforcement Decree to add enumeration clause for linking employee insurance information, medical institution usage history, passport information such as visa issuance, and immigration records. Bucheon City's intelligent epidemiological system is preparing to revise Article 32-2 of the IDCPA Enforcement Decree to add enumeration provisions on location and image data provided by data subjects.

As aforementioned, the EISS links and combines personal data from diverse sources to analyze individual locations by time and perform automated personal data processing to predict the risk of infectious diseases. This can be seen as a process corresponding to profiling defined in the GDPR. If the system automatically performs the procedure of "deciding" close contacts, who are subject to legal obligations such as self-quarantine without human intervention, it can be said that it is a solely automated decision-making based on profiling.

The nature of the personal data processed by the EISS becomes an issue at this time. According to the PIPA in Korea, legally sensitive information includes information on ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sexual life, and other personal information (Article 23), DNA information, data that constitutes a criminal history record, biometric information, and information revealing racial or ethnic origin (Article 18 of the Enforcement Decree). In the case of health information, it is noteworthy how the GDPR broadly interprets to mean "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."

Route information does not fall under the sensitive information listed in the PIPA by itself. However, the individuals who are subject to the EISS processing are confirmed patients and contacts with present and future health status already exposed including the specific name of disease, COVID-19. Hence, this can be seen as sensitive information. The PIPC has decided that personal data such as the data subject's name, address, and phone number is also considered sensitive information if the health status of the data subject with a disability can be specified (Resolution 2021-110-020). The GDPR includes information about a person collected in the course of the registration for, or the provision of, health care services as health information, as well as numbers, symbols, or particulars assigned to individuals to uniquely identify them for health purposes (Preamble 35).

In particular, contact route information can sufficiently be categorized as health information since it is processed for the purpose of identifying the health status of infection in the past, present, or future. The Austrian supervisory authority for data protection ruled that the negative PCR test results of COVID-19 were also health information in their decision on February 15, 2021.

On the other hand, if the ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sexual life, and other personal information is revealed in the route information of confirmed patients or contacts, it is clearly sensitive information. In fact, when the routes of the confirmed cases were disclosed in 2020, their information about religious gathering attendance, political assembly attendance, labor union rally attendance, and sexual orientation were exposed. This resulted in social criticism and human rights violations. The facial recognition data scheduled to be processed by Bucheon City as biometric information also falls under sensitive information that is enumerated in the Enforcement Decree of the PIPA, which restricts its process.

In conclusion, the route information of confirmed patients and contacts can be viewed as sensitive information according to the PIPA, and the EISS is a system that processes sensitive information in an automated form, such as profiling, and can be technically operated as a solely automated decision-making system. However, the PIPA and the IDCPA do not stipulate restrictions on sensitive information profiling or solely automated decision-making, nor do they provide regulations for the rights of data subjects.

In Europe, if the GDPR is applied to the processing of sensitive information for epidemiological investigations that trace the routes of confirmed cases and their contacts, Article 9(2)(h) for preventive or occupational medicine, or Article 9(2)(i) for public health will be applied. In particular, subparagraph (i) states processing health information, which is sensitive information needed for public health, it must be necessary for the public interest. It also stipulates to provide for suitable and specific measures to safeguard the rights and freedoms of data subject, in particular, professional secrecy. On the other hand, using processed sensitive information for preventive or occupational medical purposes or for public health purposes for solely automated decision-making is prohibited in principle. Solely automated decision-making can only be carried out based on the explicit consent of the data subject or for substantial public interest with suitable measures to safeguard the data subject stipulated in the law (Article 22(4)). Additionally, as many European countries specify in their laws to consult with the supervisory authority and seek prior authorization in relation to the processing of personal data in the public interest, in relation to social protection and public health (Article 36(5)), the supervisory authorities have reviewed and demanded improvement on the introduction of personal data processing and technical systems for public health needs, tracking apps for COVID-19 contacts.

On December 17, 2020, the Italian supervisory authority ruled that the system and practice of automatically processing patient health information with programs such as Excel between regional medical institutions was illegal and fined the local government. The supervisory authority noted that the automated data processing of patients could lead to patient profiling. In response, the local government came up with a bill to legalize the practice, yet the supervisory authority demanded that it be improved as well. It was said that the bill violated the principles of lawfulness, fairness, limitation of purpose, data minimization, and security by defining the purposes of statistics, administration, and public health in a comprehensive manner without clearly distinguishing the necessary purposes. Moreover, the supervisory authority considered the legality for processing sensitive information, such as the explicit consent and choice of the data subject, should be satisfied separately if automated personal data processing, such as profiling is not absolutely necessary for the treatment purposes of the data subject.

International human rights norms, such as the UN, also require the guarantee of the rights of data subjects, when processing sensitive health data in an automated manner. In particular, it demanded transparency, quality assurance, fairness, remedies, consultation with affected individuals, human intervention, and explanation when processing health data using AI algorithms. In the 2019 "Recommendation on the Protection and Use of Health-related Data", the UN special rapporteur on the Right to Privacy pointed out that an ability to opt out must be provided to data subjects if not excluded by a necessary and proportionate law when health-related data processed electronically is mandatory information (Par. 24.5). States, especially, should regulate health-related algorithms (software or computer-based algorithms that help in decision-making and analysis related to health, such as machine learning and AI) by the following principles (Par. 34.1). First, health-related algorithms should be developed and regulated in a transparent and predictable manner. Second, health-related algorithms should meet high and specified standard of quality and safety. Third, all health-related algorithms must be fair. Fourth, data subjects harmed by health-related algorithms should be able to seek compensation. Fifth, patient and health worker representatives should be consulted before adopting health-related algorithm. Sixth, health workers should make the final care or diagnostic decision and always review the outputs of health-related algorithms. Seventh, health workers using health-related algorithms should inform data-subjects that a health-related algorithm is being used and of the risks associated and their rights. In addition, any decision made using an algorithm or AI, should be explainable to the standards of decision making under existing commitments to the rule of law (Par. 34.7).

5. Direction of EISS regulations

Epidemiological investigations that process information on health conditions, such as confirmation or suspicion of infectious diseases, are bound to be accompanied by sensitive information processing under the PIPA. Sensitive information can be processed when the consent of the data subject is obtained separately from the consent to the processing of other personal information or when other statutes require or permit the processing of sensitive information (Article 23(1)). According to the Constitutional Court, even if it is permitted in Article 18 of the PIPA to use sensitive information outside of the purpose and provide it to a third party, it must fall under “inevitable case”(Case 2014Hun-Ma368). If there are special regulations stipulating the purpose and scope of processing sensitive information in the IDCPA, legitimate processing of sensitive information is possible. Currently, the request and provision of information for epidemiological investigations are based on Article 76-2 of the IDCPA and its subordinate laws.

However, the IDCPA as well as the PIPA do not have specific provisions that can regulate automated processing of sensitive information in the EISS, namely, profiling or solely automated decision-making. Nevertheless, the general provisions (Article 76-2) on the request for provision of information for epidemiological investigation is presented as the legal basis for the current EISS. The in-depth EISS or intelligent epidemiological system also seek to secure lawfulness of their expansions by additionally enumerating personal data of the collection target and related systems in subordinate statutes.

Nevertheless, the EISS, which conducts epidemiological investigations automatically, processes the personal data of confirmed cases and their contacts of infectious diseases in a way that is at higher risk than the general personal data processing method. The EISS automatically analyzes individual movements and predicts the risk of infection by linking and combining sensitive information from multiple sources. This corresponds to the process of profiling of sensitive information. In view of the current automation trend, AI functions may be used in the future to solely automate decisions that take place automatically without human intervention. The EISS plans to go beyond the temporary limit of a system targeting COVID-19 and expand to general infectious diseases. Meanwhile, the intelligent epidemiological system will be designed to process sensitive facial recognition data on its own for an indefinite number of people in street CCTV images, de-identify real datasets, and make them available for the AI industry.

The impact on the fundamental rights of data subjects will inevitably increase when the epidemiological investigations that process sensitive information have changed from manual confirmation of individual official documents to using a system with automated personal data processing; when the number of sensitive information and data subjects are increasing along with the number of linked files of personal data; with the previously closed public administrative networks added to the system; when it will be able to make solely automated decisions on data subjects in the future; and when the system is used outside its original purposes including the situation in which the personal data files built for epidemiological investigations are opened for the AI industry. In that regard, it can be said that it is unconstitutional to have no specific legal restrictions or protection measures for the establishment and operation of the EISS. This is also in contrast with the fact that the IDCPA relatively stipulates the purposes and scopes of treatment for the integrated vaccination management system (Article 33-4) and the integrated infectious disease management information system (Article 40-5).

Ultimately, it would be desirable to have provisions governing automated processing and solely automated decision-making, such as profiling, in the PIPA, the general law on personal information processing. However, considering that the EISS accompanies the processing of sensitive information and that the

IDCPA is a special law for the purpose of preventing infectious diseases and preventing the spread of infections, it seems necessary to specify in detail the purpose, scope, and restrictions of the automated processing in the IDCPA.

The purpose of automated processing of the EISS should be more specific than “if necessary to prevent infectious diseases and block the spread of infection” (Article 76-2 of the IDCPA) which is comprehensive at best. The detailed purpose of the inevitable automated processing for the public interest should be stipulated with the target and the storage limitation proportionate and minimized according the purpose. It is constitutional to disallow the use and provision of sensitive information that is not proven to be inevitable in the public interest, even if it is de-identified. When an unspecified number of people are targeted to track confirmed patients and their contacts in street CCTV images, remotely processing the facial recognition data, which is sensitive information in itself, is not inevitable, and it is an excessive infringement of fundamental rights to the data subject. Hence, it should be banned in principle.

Furthermore, there should be explicit regulations to guarantee the rights of data subjects from automated processing, such as profiling, of sensitive information. It is necessary to explain the existence, logic, and consequences of automated processing of personal data, such as profiling, to the data subjects, including confirmed patients, and ensure the data subjects with the rights to express their points of view and objections to the consequences. Guaranteeing the rights of data subjects who object profiling may also be considered. In principle, it is desirable not to allow solely automated decision-making through EISS without human intervention for sensitive information.

6. Conclusion

Korea’s response to COVID-19 is represented by the 3T (Test-Trace-Treat) Policy and includes swift and detailed tracking of subjects that is difficult to find anywhere in the world. The Korean government also expressed its ambition to promote the so-called K-quarantine model as the global standard.

“K-tracing” boasts high speed, almost close to real-time, and encompasses a close and vast range. It perpetually links major daily-life components such as resident registration numbers that uniquely identify every person from birth to death, communication, and finance. Furthermore, real-time identification must be electronically possible for implementation. Since an authoritative national identification system and advanced technology need to be realized simultaneously, it is not a global model that can be generalized.

Moreover, as pointed out by the NHRCK, there has been controversy over violations of digital rights regarding excessive collection and disclosure of personal data during detailed tracing of confirmed and suspected cases of COVID-19. Patients and their contacts whose personal data and movement were disclosed were also subject to hate speech or human rights violations. In particular, the quarantine authorities frequently collected and used location data of mobile phones carried by almost all citizens at all times. When confirmed cases occurred at LGBTQ clubs on May 2, 2020 in Itaewon, the Seoul Metropolitan Government requested and was provided with the data of more than 10,000 people with records of accessing the local base station automatically every 30 minutes during the night time from April 24 to May 6, 2020 (two weeks). The quarantine authorities was also provided with a list of 50,000 attendees for the Gwanghwamun rally held on August 15 using access information from the base stations.

Korean citizens have accepted epidemiological investigations based on detailed tracking by the government in a state of sudden emergency called the COVID-19 crisis. However, concerns about the disclosure of routes grew as well. If the risks of infringement on personal data and privacy continue to rise, the level of cooperation for epidemiological investigations might drop. Despite close tracking, the cases of unidentified COVID-19 infection routes have increased, calling for a need to re-evaluate the validity of epidemiological investigation based on close detailed tracing. In that regard, it is questionable whether the civil society will continue to accept the EISS in the future as it continues to expand its processing targets and become more automated with AI.

It is time for an approach to appropriately seek the balance between the public interest of epidemiological investigations and individuals’ digital rights. As the central government and local governments plan to expand the EISS beyond COVID-19 to general infectious diseases, and worse, use it to track people for other purposes beyond infectious disease response, regulations should be prepared to control this form of personal data processing and system and ensure the lawfulness and proportionality.

The current IDCPA and provisions of its subordinate statutes, which do not specifically limit the purpose and scope of automated processing of sensitive information, cannot be viewed as legal grounds when the state operates the profiling system that automatically processes these sensitive data. Futhermore, the lawfulness of system expansion cannot be satisfied by simply enumerating subjects in the relevant laws or enforcement decrees. It is unconstitutional to not specify clearly the purpose of public interest for automated processing of sensitive information that limits the fundamental rights of the people and the proportional measures which protects the data subject and ensures the exercise of that right.

COVID-19 is a global crisis experienced concurrently with the world, and the state measures in response to infectious diseases need to be implemented in an effort to further comply with international human rights norms.

The state and local governments need to review the appropriateness and invasiveness of the means as well as the sufficiency of safeguards to protect rights in the execution and planning of personal data processing for the purpose of responding to infectious diseases. Additionally, considering the “new normal” of our daily lives in the future after COVID-19, it is necessary to prepare legal and institutional measures to ensure digital rights from automated personal data processing and decision-making that have emerged in the real world.

* end *