Analysis on the Possibility of Electronic Surveillance Society in the Intelligence Information age

*[1]Choong-Sik Chung
Professor. Dept. Public Administration. KyungSung University, Korea. cschung@ks.ac.kr

Abstract

In the smart intelligence information society, there is a possibility that the social dysfunction such as the personal information protection issue and the risk to the electronic surveillance society may be highlighted. In this paper, we refer to various categories and classify electronic surveillance into audio surveillance, visual surveillance, location surveillance, biometric information surveillance, and data surveillance. In order to respond to new electronic surveillance in the intelligent information society, it requires a change of perception that is different from that of the past. This starts with the importance of digital privacy and results in the right to self-determination of personal information. Therefore, in order to preemptively respond to the dysfunctions that may arise in the intelligent information society, it is necessary to further raise the awareness of the civil society to protect information human rights.

Keywords*: ICT, Electronic Surveillance, Information Society, Digital Privacy, Information Human Right.*

Ⅰ. Possibility of Electronic Surveillance Society

Now the world has entered into smart intelligence information society by the development of advanced ICT. These smart information societies evolved more from the global network called "Information Village" in the past, so that the world is connected in real time and its complexity is further increased. Therefore, with the development of ICT, the breadth, speed and interdependence of the changes have increased, and the risk factors of society are also increasing. Therefore, in the smart intelligence information society, there is a possibility that the social dysfunction such as the personal information protection issue and the risk to the electronic surveillance society may be highlighted.

In particular, there is a possibility that the extent of infringement of personal information by corporations as well as the surveillance of individuals in the nation may spread rapidly, considering the recent information gathering behavior of large multinational corporations such as Google, Apple, and Facebook. In this way, if personal surveillance by corporations and state powers is accelerated by the rapid development and convergence of information technology in smart information society, ultimately it will face government distrust and national trust crisis. Therefore, in order to preemptively cope with this situation, this paper aims to examine the emergence of a smart electronic surveillance society from the perspective of the social change paradigm.

II. The Emergence of Intelligence Information Society

Today, the world we live in is preparing to evolve into a new paradigm of smart intelligence information society based on ubiquitous and intelligent communication technologies. The emergence of smart intelligence information society will bring revolutionary results in all areas, not just changes in technological development and changes [1].

As information technology becomes more sophisticated, knowledge and information become more and more intelligent, new information communication technology and traditional industrial

* Corresponding Author
Received: Sept. 27, 2018, Revised: Nov. 27, 2018, Accepted: Dec. 26, 2018

technology are merged in various ways, and smart new technology, that is smart information technology, is emerging. This smart information technology is a driving force for social change. So we will briefly review the changes in social paradigm.

2.1 Social Change due to ICT Development

Increasing inter-state interaction, increasing complexity, convergence of technologies and integration of services in accordance with globalization are factors that accelerate social change. The period of transition from agricultural society to industrial society took 6,000 to 7,000 years. But it was only 250 years less than 1 / 20th of what it would be like to convert from industrial to information society. In addition, this information society has evolved into a smart intelligence information society through the convergence of information and communication technology (ICT) beyond the nano-bio society.

Information technology is rapidly changing into smart information technology, which is fused with ubiquitous technology, and even objects have intelligence. Therefore, the value of human-centered creativity and flexibility is becoming more important based on the information society value of sharing and openness. Changes in smart information technology and social core values are evolving human history from information society to smart intelligence information society.

Smart intelligence According to the emergence of information society, the type of industry such as mobile related industry, activation of one company is changing variously based on these technologies and values. Rapidly developing information and communication technologies are also increasing the possibility of electronic surveillance for individuals.

2.2 The Emergence of Artificial Intelligence and Electronic Surveillance Society

The debate over the electronic surveillance society has long started. But now, smart information technology has made it different. Smart Intelligence in the information society, all work processes are processed in digital form in virtual space, leaving audit trails. Therefore, in the smart intelligence information society, it is highly likely that the electronic surveillance using the intelligence information described above is generalized. The arrival of the intelligence information society by the information technology revolution inevitably predicts a new level of social monitoring and control. The information processing technology of digital artificial intelligence is accompanied by an increase in surveillance ability in various ways.

Specifically, from the technical perspective, surveillance technologies such as information communication technology, biometrics technology, biotechnology, and remote surveillance technology have developed remarkably. With the development of information processing technology including Big Data, The cost, speed, and accuracy of storage have been greatly improved. These advances in information technology have allowed nearly unlimited information gathering, processing, and storage while maintaining high accuracy at low cost. As a result, the amount and quality of information collected, processed, and stored has increased and become greater than can be compared to 10 years ago. And today, the trend of increase is very explosive, as we are entering the era of intelligence information based on Big Data [2].

III. New Forms of Electronic Surveillance Technology

As information technology environments, which affect the development of surveillance such as smart phones and ICT, rapidly developed, surveillance technologies are becoming refined and advanced [3]. In Wikipedia, the types of surveillance are classified as follows: computer, telephone, camera, social networking analysis, biometrics, aerial surveillance, data mining and profiling, human operative, satellite imagery, identification and credentials, RFID and geolocation devices, biomedical chips, human microchip, covert listening devices & video devices, postal services surveillance, and stakeout and so on. The type of surveillance presented in Wikipedia is believed to cover almost all types of surveillance that currently exist. However, methods, subject, and technique of surveillance are mixed.

In this paper, we refer to various categories and classify electronic surveillance into audio surveillance, visual surveillance, location surveillance, biometric information surveillance, and data surveillance. Acoustic surveillance includes wired and wireless telephone tapping and room tapping as well as existing categories. Video surveillance includes ultra-small cameras (near),

CCTV and black box (medium distance), manned and unmanned aerial photography (long distance), and satellite photography (grassland distance).

Location monitoring includes devices and technologies used to identify location information such as GPS, smart phones, and RFID. Biometric information monitoring includes fingerprint, iris, finger vein, face, voice, and the like. Data monitoring includes digitized data such as Internet use, SNS use, and resident registration number.

3.1 Audio Surveillance

Acoustic surveillance is a form of surveillance that uses microphone and recording technology to hear or record conversations from third parties. Eavesdropping is a typical case of acoustic surveillance. SECTION 2 (DEFINITION) OF COMMUNICATION SECURITY PROTECTION LAW 7 defines the supervision. According to this, without the consent of the parties to the telecommunication, it is possible to listen to and read the sounds, texts, codes and images of the communication by using the electronic devices, . In the case of eavesdropping, it is referred to only as illegal, but in case of eavesdropping it includes both legal and illegal cases.

Smart phones, smart home appliances, etc. are becoming popular. As the functions of smart devices equipped with voice recognition become more sophisticated, there is a concern about the sound monitoring. It is argued that Smart TV, which will be spread to all households in the future, can record and provide all the conversations in the house. In this case, the smart home will be able to become a smart prison with smart electronic surveillance.

3.2 Visual Surveillance

Video surveillance is a method of grasping the shape, behavior, and location of the surveillance target using cameras, photo shoots, and video recording techniques. With the advancement of optical technology, cameras have become more sophisticated, smaller, and lighter, enabling them to acquire high-quality images through aerial photography and satellite photography as well as when installing video surveillance devices such as glasses and drums. In addition, various levels of video surveillance devices have appeared, and the cost of operating the video surveillance system has become low, so that not only the government, enterprises, but also individuals are installing and operating video surveillance devices according to their purposes.

A typical technology of video surveillance is CCTV (closed circuit television). CCTV installation status, popularization, growth of market, etc. are typical examples showing how much the video surveillance system has spread to our lives. In addition to CCTV, video surveillance systems are operating various video surveillance systems such as drone equipped with surveillance equipment, satellite photographing, aerial photographing, and car black box. In the first place, black boxes for cars were introduced to secure evidence of traffic accidents, but there are side effects that are misused and misused. In this situation, most residents in major cities are exposed to video surveillance system in most of the daytime activities, and even private spaces such as the home can be exposed to video surveillance according to the intention of the surveillance system.

3.3 Location Surveillance

The field of location surveillance has recently become one of the most vigorous areas of development combined with corporate marketing activities. Here, the location information of the individual who is subject to privacy protection is distinguished from the general personal information and the following three points.

First, the location information of the individual is dynamic information. General personal information such as name, resident registration number, and address is static information that is maintained for a relatively long time. On the other hand, position information is dynamic information that continuously changes with time, Path, and time of change are very important. In the location information, it is important to record the movement trajectory of the user by tracking or linking the changed location information, not merely on the specific position of the past or present point in time.

Second, the location information of an individual is sensitive information. The location information, especially the location information of the individual, can be said to be sensitive information which may cause remarkably serious consequences compared to other personal information in case of unauthorized leakage. The location information not only informs the past and current location of the individual, but also can predict the future location of a certain level by

using the direction of the location information and the data mining technique for processing various information.

Third, the location information of the individual is very likely to be used for public purposes and industry. First, location information can be used mainly for public interest purposes such as public emergency structure, traffic information, and weather information. The current location information law also requires the use of personal location information for emergency rescue (Chapter 4) since the enactment in 2005.

3.4 Biometric Information Surveillance

First, biometrics has been defined so far. The definitions of biometrics and biometric information are summarized as follows. Biometrics can be used to identify individuals using the unique characteristics of a person's body (fingerprints, iris, retina, vein, palm, face, etc.) or behavioral characteristics (voice, handwriting, body shape, gait, Technology. Such biometrics should be easy to acquire and quantify by sensors (universal character, uniqueness), permanence (unchangeable and unchangeable character), acquisition Characteristics) are required.

Biometrics technology, which identifies the identity of a person through the combination of human biological characteristics and ICT technology, is rapidly replacing the existing password-based personal identification and authentication system. Biometric technology, which verifies the identity of an individual with body data, .

Based on the security and convenience of biometrics, it is widely applied as a means to prevent identity verification, illegal use of the system, and electronic payment of unauthorized methods in the fields of finance, communication, security, automobile and medical care.

Biometrics technology has various technologies such as fingerprint recognition, iris recognition, vein recognition, face recognition, voice recognition, hand recognition, etc. Unlike existing passwords (authentication certificates, security cards, OTP, SMS authentication) · There is an advantageous aspect in terms of low risk of forgetting, very high security, and convenience.

3.5 Data Surveillance

In recent years, most of the issues of smart electronic surveillance in the intelligent information society have arisen in the field of data surveillance. The main subject of data surveillance has been the government in the past, but now it is rapidly expanding into corporations and individuals [5]. Our everyday life can be abundantly developed through the implementation of intelligent information society through data monitoring and big data analysis. On the other hand, there is a rosy outlook on the infinite benefits that Big Data will bring, but on the other hand, there is a fear that the government will sneak into my smartphone messenger and sell out my personal information [6].

Many people have long since compared the Internet to the sea of information. On the Internet, where users can find unimaginably large amounts of information, they all use search sites. Both Google, which is widely used in the world, and NAVER, which is widely used in Korea, automatically generate and collect the user's IP address, cookie, use date and time, and usage log.

In addition, social network service (SNS) data such as Twitter and Facebook are also being watched by electronic surveillance. In particular, companies are increasingly asking for applicant's SNS information when recruiting new employees. Also, after the recruitment, it is reported that the number of companies that are looking at the employees' SNS is also increasing. As such, it is the individual's interest in looking at the SNS, but looking at the SNS from the country is ultimately a matter of electronic surveillance.

IV. Policy Advice for Electronic Surveillance

Recently, the majority of smartphones being sold in Korea are providing identification functions through fingerprints and iris. Thus, a new paradigm of electronic surveillance will be created when biometrics becomes a means of identification. Therefore, in the future, biometrics will be used in almost all fields, whether public or private.

In the end, however, the activation of biometrics throughout society will create an environment in which personal privacy can no longer be maintained. Therefore, countermeasures against the proliferation of smart electronic surveillance society should be prepared in advance. In this section,

we will examine the changes in perception, the current status of laws and systems, and policy measures in response to the arrival of this smart electronic surveillance society.

In order to respond to new electronic surveillance in the intelligent information society, it requires a change of perception that is different from that of the past. This starts with the importance of digital privacy and results in the right to self-determination of personal information.

4.1 Digital Privacy

'Digital privacy' is becoming more important because of the various ICT technologies used in the intelligent information society. In other words, the contents of privacy are changing due to the rapid infringement of personal life through the utilization of technology different from the past. In particular, the importance of personal information that can identify an individual in a virtual space has been emphasized. Until now, it was important to prevent the leakage of personal information in relation to privacy. However, now, in order to utilize various social network services (SNS), more personal information should be disclosed and utilized. Especially, in the hyperlinked society where the internet and the artificial intelligence are combined, there is a conflict with the privacy because they pursue the openness of the information according to the social connection and the autonomy of the individual.

Therefore, a new digital privacy standard should be applied to the generations that disclose all of these things. In such an intelligent information society environment, individuals will actively determine their disclosure level by distinguishing their personal information between the increase of personal information utilization and the possibility of personal privacy invasion.

4.2 Right to Be Forgotten and Request to Delete

Digital privacy, as we have already seen, has been shown to be a right to be forgotten and a right to delete. This right to be forgotten has begun in Europe, became a global concern after the European Court of Justice ruling in May 2014. Currently, the right to be forgotten is being raised as one of countermeasures against various personal information leakage and proliferation of intelligent information society, and discussion is ongoing. In the digital environment where information sharing is widespread, various constitutional issues are being raised on the institutional merits of ensuring the right to remove information about individuals' personal information and prevent them from being searched.

Now, in order to strengthen privacy in the intelligent information society, it is necessary to understand ‘'right to be forget’ from the viewpoint of new fundamental rights. As the information privacy rights or personal information self-determination right that have been developed so far are difficult to completely protect all types of personal information and the “right to be alone” right of privacy in the late 19th century was newly argued, A new type of privacy right is needed, just as it was done in major countries around the world.

4.3 Right to Explanation: Regulation of Algorithms

The rights of the digital privacy perspective discussed above are now evolving into the right to demand explanations in the intelligence information society. Recently, as the artificial intelligence technology and services have been widely spread, the production and distribution of information has become possible by artificial intelligence algorithms, not by people. However, as a reaction to the industrial advantage of artificial intelligence, discussions are being actively made to standardize the 'algorithmic accountability' or 'algorithm transparency' as a normative response to technological and social adverse effects or dysfunctions of artificial intelligence have.

The starting point of such a discussion is that artificial intelligence algorithms are not fair and neutral, but that the selection of specific algorithms or algorithm - based decision making results in discriminative and exclusionary results. For example, as has been the case in recent US presidential elections, it is a concern that Google and Facebook's recommendation and search algorithms may lead to politically biased public opinion. Thus, the US Obama administration has warned that a widely commercialized Big Data Analysis algorithm can cause social prejudice and distortion, especially gender discrimination and racism.

Therefore, since the algorithm is constituted by human judgment or selection, it is necessary to contain bias and differentiation. Therefore, it is naturally necessary to regulate the algorithm design, development and utilization process. A full discussion of algorithmic regulation has recently been published in the European Union (EU)

The General Data Protection Regulation (GDPR) has to deal with the 'algorithmic transparency', including 'right to explanation' for automated personal decisions such as profiling. . Algorithms are becoming more and more important as social monitoring and regulation in the 'public domain' rather than 'machine domain', which simply operates automatically [7].

V. Conclusion

The intelligence information society triggered by the Fourth Industrial Revolution has both light and darkness. Until now, we have pursued only rosy utopia, but in reality, the dysfunction of intelligent information society is also manifested in various ways. Therefore, countermeasures against the proliferation possibility of smart electronic surveillance society should be prepared in advance.

5.1 Information Human rights in Intelligence Information Society

Human rights are the fundamental and irreversible fundamental rights that an individual enjoys as human beings, so that human dignity can be respected and realized. The State is obligated by the Constitution to ensure and guarantee such human rights. Article 10 of the Constitution states that “all citizens have the dignity and value as human beings and have the right to pursue happiness”. The State has the obligation to confirm and guarantee the non-inviolable human rights of individuals. It is collectively referred to as "Information and Communication Technology and Human Rights". On May 26, 2005, the Constitutional Court ruled that there was a need to constitutionally approve the right to self - determination of personal information as a new fundamental right.

The National Human Rights Commission defines the information human rights as follows. "Information and Communication Technologies (ICTs) and Human Rights" means the process of collecting, processing, distributing, and utilizing digitized information by information and communication technology, and the resulting information value to undermine human dignity. Basic rights can be used freely and without discrimination.

In order to protect personal information from the risks inherent in the development of modern information and communication technology, ultimately it would protect the freedom of individual decision. It is a minimum constitutional safeguard necessary to prevent the possibility of total damage to the foundation of the Constitution.

5.2 Strengthening Information Privacy

Information privacy (or Data Privacy) is the right of an information entity to control information about himself / herself that may affect privacy. Since privacy violation is achieved by collecting, using, providing and distributing personal information, information privacy rights issue ultimately results in the collection, use and control of personal information. In this sense, information privacy has differentiation from traditional sense of privacy, which has emphasized the freedom of the individual's private life, ie, the exclusion of interference with the body, space and decision - making.

The contents of the personal information self-control which constitutes the core of information privacy right are as follows: the right to collect and use personal information, the right of withdrawal of consent, the right of correction and deletion, the confirmation of processing of personal information, And the like. In addition, many countries' legislation emphasizes the anonymity of personal information processing. However, since anonymity is generally recommended, it has not yet developed into the rights of information entities.

As the intelligence information society becomes more and more sophisticated, much of its life depends on smartphones and information and communication technologies. Even if it is not visible, the influence of information surveillance by governments and corporations is increasing. Especially, the uncontrolled government's oversight of the power of surveillance is likely to lead to abuse of the state power based on the collected information, and to human rights violations such as social discrimination and disadvantage [8]. Therefore, in order to preemptively respond to the dysfunctions that may arise in the intelligent information society, it is necessary to further raise the awareness of the civil society to protect information human rights.

VI. Acknowledgments

This research was supported by Kyungsung University Research Grants in 2018.

VII. References

[1] S. G. Han. “Societal Impact of AI”. 「Presented at KAPAE 2016 Spring Symposium」. May 13, 2016.
[2] FTC. “Big Data, A Tool for Inclusion or Exclusion?”, January, 2016.
[3] UNDOC. Current Practices in Electronic Surveillance. 2009.
[4] Woolf, Nicky. “How to solve Facebook’s fake news problem: experts pitch their ideas“, The Guardian. November 26, 2016.
[5] Lyon, David. The Electronic Eye -The Rise of Surveillance Society. Basil Blackwell Ltd. 1994.
[6] Executive Office of the President. “Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights”, May, 2016. USA.
[7] W. T. Lee. “EU Algorithm Regulatory Issues and Policy Implications”. KISDI Premium Report. 16-12. KISDI. December 26, 2016.
[8] Garfinkel, Simon. Database Nation: The Death of Privacy in the 21st Century, O’Reilly & Associates, Inc. 2000.