Journal of The Korea Society of Computer and Information
Vol. 20 No. 7, pp. 109-114, July 2015

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.7.109

The Protection of Personal Information and the Principle of Proportion in Information Societies

Hyung-Keun Gu *

Abstract

With the realization that the police's personal information gathering activities can violate the authority to decide one's information guaranteed by the Constitution, many people are interested in the legal terms of the police's information gathering and handling. The police's personal information gathering activities imply both the purpose of public welfare and order and the risk of violation of basic rights of citizens, their effective balance is critical. In this respect, this study reviews the principle of proportion as a principle of control of personal information gathering and handling (police intelligence activities) by state to discuss its implications on legislation.

▸ Keyword :The authority to decide one's information, The protection of personal information, The principle of proportion, Principle of necessity, Information Societies

Ⅰ. Introduction

The major duty of the police is to maintain public wellbeing and order, and the police have gathered the necessary information for effective performance of duties through questioning, monitoring, and other means. Unlike the past, however, information processing technology have developed exponentially to create a society where large quantities of personal information can be gathered and processed in various ways, and personal information gathering and processing by a state office, especially the police, cannot avoid controversies in terms of the basic rights of citizens.

In other words, personal information gathering and processing by state can be seriously risky for the freedom and reputation of individuals as it often takes place in secrecy without any notice to the individuals.

Police intelligence activities requires strict and specific legal regulations, but the current legal system in Korea does not offer any uniform regulations.

Therefore, it is very important to control personal information gathering and processing (police intelligence activities) by legal measures, and it is urgent to improve the legislative control in terms of protection of personal information in regards to personal information gathering and processing by state.

The purpose of this study was to discuss the principle of proportion as the principle of control over personal information gathering by national authority and to suggest the basic directions for legislation in regards to personal information gathering and processing by state.

First, it discusses the general legal principles of personal information control and the application of authority to decide one's information and the police's legal systems as the constitutional evidence of legal restrictions over the police's personal information gathering and processing.

• First Author: Hyung-Keun Gu
*Hyung-Keun Gu (younbal89@hanmail.net), College of General Education, Chosun University
• Received: 2015. 07. 04, Revised: 2015. 07. 07, Accepted: 2015. 07. 11.
• This study was supported by research fund from Chosun University, 2014

Then, it clarifies the current legal evidence of personal information and its limitations based on the general theory of law. It particularly discusses the principle of proportion as a principle of protection of personal information of the police that needs to be observed for the legislation of police activities in regards to personal information and is important in terms of interpretation, and suggests the possible improvement measures.

II. Police Intelligence Activities

1. Concept

Police intelligence activities refer to the police activities for the prevention of all legal activities of individuals or organizations that invades the safety of state. Specifically, they refer to gathering personal information of all suspects for public wellbeing and order[1]. The major topic of discussion in regards to police intelligence activities is the personal information, which includes personal information that can identify individuals such as name, place of birth, age, address, phone number, and physical characteristics, and property information related to certain individuals.

2. Types

2.1 Gathering and storing information

Police intelligence activities refer to all activities of gathering personal information of a certain natural person for the purpose of police activities. Recognition and documentation of personal information are forms of information gathering. Information storing refers to keeping in the information box or copying for continual use.

2.2 Managing information

Managing information generally refers to gathering resources to extract and store information and to change, use, delete, and block it as needed.

2.3 Providing information

Providing information refers to providing or granting access to a third party the information directly acquired by storing or processing. The form of providing information includes verbal and writing[2].

3. Need for control

Police information gathering and processing by state can be seriously risky for the freedom and reputation of individuals as it often takes place in secrecy without any notice to the individuals.

As large amount of information can be stored in the digital age with the development of scientific technology, personal information can be gathered limitlessly, downgrading citizens into mere source of information.

Therefore, police intelligence activities should be supported by strict legal grounds with legislative control.

4. General Principles

Police intelligence activities often takes place against one's will or without any notice. Therefore, police intelligence activities should comply with a few strict principles.

4.1 Direct information gathering

Police intelligence activities should gather personal information directly from each individual.

Each individual should be able to know by whom, about what, when, and for which purpose their information is gathered and processed. The principle of immediacy is derived from the authority to decide one's information that each individual can decide whether their information can be provided and used.

However, there can be an exception when it is impossible or excessively inefficient to gather information from each individual. Information gathering from a third party is allowed only in special cases defined by law[3].

4.2 Open information gathering

Police intelligence activities should be open and transparent as they take away the chance of self-defense from the people whose basic rights are violated for a long time when they take place in secrecy.

Therefore, information gathering through long-term surveillance or video-taping in secrecy is prohibited in principle, except for inevitable cases where open information gathering cannot achieve purpose.

4.3 Principle of notification

If personal information is gathered from an individual or a third party, the provider should be appropriately notified of the legal grounds of information gathering, whether information will be provided, and purpose of

using information.

The principle of notification is an important element of transparency along with the principles of immediacy and openness.

4.4 Principle of anonymity

When it comes to police intelligence activities, an appropriate level of anonymity can limit excess gathering of information. Even if personal information is gathered and stored lawfully, personal identification should be minimized when it is used and provided to prevent violating the basic rights of citizens[4].

III. Protection of Personal Information

1. Significance

Each individual has the right to manage and control their own information and decide whether to disclose it. This right is known as the authority to decide one's information.

The authority to decide one's information refers to the right of each individual to decide when, to whom, and to which extent their information should be disclosed and used.

It also includes the right to demand disclosure and modification of personal information on the database[5].

2. Constitutional grounds

In case of Germany, there is no federal provision that secures the authority to decide one's information, except for the constitutions of some states that explicitly specify the basic rights for the protection of personal information. However, the theories and precedents of Germany derive constitutional grounds from personal rights.

In case of Korea, there are conflicting opinions.

A number of theories look for the grounds of authority to decide one's information in the freedom and secrecy of privacy in Article 17 of the Constitutions, but some theories refer to the provisions on human dignity and value in Article 10 of the Constitutions.

However, the opinion that looks for the authority to decide one's information in Article 10 of the Constitutions interprets the scope of protection of freedom and secrecy from a perspective too narrow. The legal nature of freedom and secrecy of privacy is primarily the right of freedom with a passive and defensive character, but the scope of protection can be broader from the perspective of protection of personal information based on Article 17 of the Constitution.

Article 17 of the Constitution can claim prohibition of random gathering and processing of one's information by state and compensations in case said clam is not accepted[6].

3. Limitations

The authority to decide one's information is not guaranteed absolutely. Individuals do not exist in isolation, but as members of social communities. Even if information is about an individual, it is not exclusively vested oneself. Also, personal rights of community should be restricted for the safety and order of social communities.

Therefore, each individual's authority to decide one's information can be restricted for the dominating public welfare in principle.

What should be remembered here is that the benefit of a social community does not always justify the restriction of authority to decide one's information. It is important to consider where the authority to decide one's information should be allowed and how the regulations should be established[7].

The restriction of authority to decide one's information must be supported by explicit grounds by law, and legislators should comply with the principle of proportion. The legal grounds of police intelligence activities on personal information are required to be stricter than other areas.

IV. Application of the Principle of Proportion

Police intelligence activities on personal information should first consider the authority to decide one's information and then the principle of proportion for its restriction for public benefits.

There should be a reasonable proportional relationship between the public benefits achieved by police intelligence activities and its violation of personal benefits. The principle of proportion was originally established to limit the police authority with common sense, but the principle of proportion today is admitted as a constitutional principle derived from the principles of a

constitutional state rather than a mere principle of common sense[8]. Its specifics are as follows.

1. Suitability

Police intelligence activities should be suitable for maintaining public wellbeing and order, and their execution should be permitted by law. The purpose of gathering personal information is permitted within the scope of purpose in order to satisfy the condition of suitability. Here, purpose should be specified based on the void of vagueness so that the general public can know why their personal information is gathered by law.

Also, storing and using personal information are permitted within the scope of purpose of gathering. Therefore, personal information should be provided to third party for the specified purpose only.

If it is proven later that police intelligence activities are not suitable for achieving purpose, police intelligence activities should stop, and the actions taken already should be undone.

2. Principle of Necessity

The principle of necessity states that personal information gathering by police intelligence activities should be limited to the information for public benefits. In other words, only the information actually required for public benefits should be gathered, and extensive personal information gathering unrelated to public benefits should be prohibited. Also, personal information unrelated to public benefits should no longer be gathered or used, and all stored personal information should be destroyed.

Personal information gathered by police intelligence activities should ensure public benefits and used within the scope of purpose of public benefits[9].

3. Principle of Reciprocality

The principle of reciprocality states that even police intelligence activities for the purpose of public benefits should ensure that the public benefits are dominating when compared to the private benefits of individuals sacrificed.

The issue is the comparison between the public interests achieved by personal information gathering and the sacrifice of each individual.

When it comes to police intelligence activities, the violation of public freedom and rights should be strictly compared with the public benefits acquired, and all citizens should accept it if the public benefits are dominating[10].

What is important here is that police intelligence activities are permitted only in the scope of certain purpose by law.

The purpose of public benefits, including the subjects and conditions, should be specified for the void of vagueness so that it is clear for all citizens.

4. Order of application

The three aforementioned principles should be applied in the following order: suitability, necessity, and reciprocality. In other words, only the necessary measures among the suitable measures should be used only when they satisfy the principle of reciprocality. If the level of suitability is equivalent to the level of necessity and reciprocality, the selection should be based on the police judgment.

5. Legislative rules

The authority to decide one's information can only be limited by dominant public benefits. Also, personal information gathering should be suitable for the purpose of public benefits.

For this purpose, first, the legislator should clearly state the subjects and conditions of police intelligence activities within the principle of proportion. In this case, the types of personal information and the method of gathering should be specified explicitly. Gathering personal information should be prohibited if it is unclear or not anonymous for future purposes[11].

Second, the permission to and condition of gathering private information should be determined carefully. Private information conflicts with the authority to decide one's information, so it should be gathered openly in principle, unless it is strictly permitted by law in exceptional cases where public benefits cannot be secured.

Third, legislators shall explicitly specify in law the obligation to delete, notify, and explain personal information gathering. The obligation to delete is basically not for the benefit of police that stores the information, but for the public benefits for the protection of personal information. Therefore, personal information should be deleted when demanded by the individuals[12].

The obligations of notification and explanation are also

critical measures for the protection of personal information. Each individual should know where and for which purpose their information is gathered by the police authority. The police should notify and explain to each individual about the personal information they have in possession.

Finally, the intervention of independent institutions should be secured by law for the protection of personal information[13].

For example, it may be considered to make reporting the personal information gathered by police intelligence activities to a supervisory organization mandatory.

Ⅴ. Conclusion

Police intelligence activities are increasing for public wellbeing and order.

Personal information is easily gathered in various ways with the development of information communications technology. However, police intelligence activities should be controlled appropriately as they always imply the possibility to violate the basic rights guaranteed by the Constitutions.

The protection of personal information is important in the information society because it is closely related to the protection of basic human rights. Also, the protection of authority to decide one's information, which is derived from the secrecy and freedom of privacy guaranteed by the Constitutions, is an important duty of state.

For this purpose, a legislative control is necessary along with strict and specific conditions for personal information gathering and processing by state, and what is considered for this is the principle of proportion.

It should be under the control of principle of proportion in order to ensure the harmony of protection of personal information and police intelligence activities.

Even if police intelligence activities are supported by legal grounds, the public benefits achieved by such activities should be greater than the private benefits sacrificed in order to justify it.

Police intelligence activities should not be permitted limitlessly for the abstract benefits of the public.

Even if an action is permitted, it should be supported by legal grounds that satisfy the principles of suitability, necessity, and reciprocality based on the principle of proportion.

The principle of proportion should be applied to legislation in order to balance police intelligence activities for public benefits and the protection of personal information guaranteed by the Constitutions.

Finally, there should be uniform regulations on personal information gathering in order to satisfy the constitutional demands to guarantee the basic rights of citizens, and legislative control should serve as the final fort the for the protection of freedom.

REFERENCES

[1]Myeung-Yeun Kim, "Der Schutz der personenbezogenen Daten im Polizeirecht," Public Land Law Review, Vol.25, p.303, Feb. 2005.

[2] Man-Hyeong Cho, "The Protection of personal Information and Principle of the Proportion in the Police Intelligence Activities," Public Land Law Review, Vol.51, pp490-491, Nov. 2010.

[3]Seong-Tae Kim, "Personenbezogenen Datenverarbeitung der Polizei," Police Law Review, Vol. 1, pp102-104, Jun. 2003.

[4] Supra Note 2, p.497.

[5] Jang-Jun Kwon, "Die Datenerhebung der Polizei und informationelle Selbstbestimmung," Wonkwang Journal of Law research, Vol. 25, No. 2, pp.308-309, Jun. 2009.

[6] Supra Note 1, pp.247-248.

[7] Supra Note 5, p.317.

[8] Byung-Doo Oh, “A Study on the General Information-gathering of the Police,” Democracy Law Review, Vol. 30. p.198, Mar. 2006.

[9] Young-Gil Kwak, "The Limit of State Regulation for Freedom of Expression in Cyberspace," Korean Review of Crisis & Emergency Management, Vol. 7. No. 6, pp.189-190, Dec. 2011.

[10] Jeong-Sun Hong, "Police Administrative Law," Park young Sa, p.363, 2013.

[11] Min-Seok Bang/Cheol-Ho Oh, "A Review of Studies on personal information," Informatization Policy Journal, Vol. 21. No. 1, pp.15-16, Jan. 2014.

[12] Il-Hwan Kim, "A Critical Review of Personal Information Protection Act Revision," Public Land Law Review, Vol. 52, pp.269-270, Feb. 2011.

[13] Pieroth, Bodo/Schlink Bernhard, “Polizei-und Ordnungsrecbt,” München, p.69, 2002.

Authors

Hyung-Keun Gu received the LL.B, LL.M. and Ph.D. degrees in Public Law from Chosun University, Korea, in 1999, 2003 and 2006, respectively

Dr. Gu joined the faculty of the Department of Law at Chosun University, Kwang, Korea, in 2006. He is currently a Professor in the College of General Education, Chosun University. He is interested in cyber-crime, intelligence police and digital policy.