Protection of Employees' Personal Information and Privacy at a Crossroads in Korea

Sung-Wook Lee*
Ewha Womans University

I. Introduction

In recent years, advancements in and supply of information and communication technologies have affected workplace order and labor relations in various ways. On the one hand, the new technologies being used in labor surveillance have changed the control of labor fundamentally, and on the other hand, employers have used these technologies to accumulate and use vast amounts of employees' personal information. In general, the employer tries to collect and use as fully as possible not only customers' information but also employees' personal information. In the collection and accumulation of the latter, the employer tries to take advantage of the employees' capacity to work. The employer is also aware that the quantitative and qualitative accumulation of such personal information itself can influence the asset value of the company.

Such collection and accumulation of employees' personal information is a way of taking full advantage of employees' ability, and therefore, having regard to the concept that the ability of quantitative and qualitative accumulation of personal information itself be employer's value of property, it is common for employers to make full effort on collecting and using employees' personal information, as well as the customers'. This change raises new issues and questions in labor law, which is established based on traditional labor relations.

First of all, as traditional methods of labor surveillance (which for the most part relied on human and bureaucratic regulations) are being replaced rapidly by electronic surveillance system,[1] several phenomena can be observed with regard to restrictions in labor relations. First, advancements in information and communication technologies has led to the continuous surveillance of employees outside the limits of work time and workplace, with the scope of monitoring expanding from public to private areas. Second, the intensity of surveillance has risen remarkably due to the growth in accessibility and

---

* Professor of Law, School of Law, Ewha Womans University, Seoul, South Korea. I am grateful to Suna Kim, JD candidate, for her invaluable research assistance.

1 Nowadays in Korea, various methods, such as closed-circuit television (CCTV), network camera, location-tracking systems (e.g. GPS [Global Positioning System], Smart Phones, etc.), remote frequency ID card (RFID card), biometric sensors equipment, business use PC, telephone, E-mail monitoring, Internet use monitoring, enterprise resource planning (ERP), etc. are used as electronic surveillance system. *See* National Human Rights Commission of Korea, *Influence of Surveillance Systems in Workplace on Labor Human Rights,* 26-36 (2005).

penetration of impersonal monitoring systems. Third, precision surveillance system has led to analysis of employees' behavior patterns, with such things as an employee's thoughts and tendencies being monitored. Integration of electronic surveillance and information system has made possible 'systematic surveillance'[2] of the workplace. Surveillance equipment using information and communication technologies can monitor employees anytime anywhere and produce data for evaluation by obtaining, recording and storing information about a person's physical activities and psychological status, thereby operating as systemic surveillance system of not only labor itself but also of employees' personalities by processing obtained data into business management information.

Such phenomenon gives rise to two problems. First, as electronic surveillance system is developed, installed, and applied at the initiative of the employer, data produced from the system can be approached and utilized by the employer exclusively. This accelerates the information asymmetry between employer and employee. As a result, not only can this weaken the basic principle of the employment law in Korea—"Terms and conditions of employment shall be freely established on the basis of equality, as agreed between workers and their employer"[3]—but it can also leave the employee susceptible to arbitrary discrimination and exclusion due to the information monopoly of the employer. Second, development of electronic surveillance system will alter surveillance from something visible to something clandestine. Employees will fail to know when, where, and how the surveillance is enacted. With the possibility of omnipresent surveillance, the workplace, where an employee's personality should be manifested through labor, is threatened to degenerate into a type of Bentham's Panopticon.[4] Considering these problems, the issue of labor surveillance involving information and communication technologies should be approached from a labor law perspective.

There are also legal problems concerning the employer's large-scale collection and accumulation of employees' personal information. In some ways, it is inevitable for employers to collect, store, and manage information about employees for optimal regulation of the labor force on the basis of employment contract in labor relations. However, conflict with employees' right to control personal information is already inherent in labor relations. Especially, as long as the information holds intrinsic value, the risk of an employer collecting, using, or leaking employees' personal information always exists. The legal approach to solve this issue should consider two important facts: because of its nature, personal information misused can cause irrevocable damages to individuals qualitatively, and also always has the possibility of causing massive damages quantitatively.

Therefore, it is necessary to create active and dynamic legal restrictions and principles for the protection of employees' personal information and privacy. This should include preventive measures as well as *ex post* relief, in consideration of the influences of rapid development of information and communication technologies on workplaces and employees.

---

[2] *Ibid*, p.15.
[3] *See* Article 4 of the Labor Standards Act.
[4] Michel Foucault, *Discipline & Punish: The Birth of the Prison* 195-228 (NY: Vintage Books) (1995).

II. Regulation Systems for the Protection of Employees' Personal Information and Privacy

A. The Constitution

Article 10 of the Korean Constitution prescribes, "All citizens shall be assured of their human worth and dignity and shall have the right to pursue happiness. It shall be the duty of the State to confirm and guarantee the fundamental and inviolable human rights of individuals." With regard to the protection of privacy, the Constitution states, "The right to privacy of all citizens shall not be infringed"(Article 17) and also explicitly guarantees the privacy of communication (Article 18). Although it does not have explicit code about the protection of personal information, the Higher Courts in Korea make it clear the wide protection of personal information by active interpretation of the Constitution.

The Supreme Court stated that Article 10 and Article 17 of the Constitution are purposed to "guarantee not only a passive right to be protected from a third party's infringement on one's privacy, but also an active right to voluntarily control information of oneself,"[5] which makes it clear that the right of privacy has both passive and active dimensions.

Furthermore, the Constitutional Court approves "*the Right to Self-Determination of Private Information*" as a new separate fundamental right. In a case arguing about the unconstitutionality of fingerprinting system of the Resident Registration Act and the actions of the chief of the metropolitan police agency storing and using fingerprint data, the Constitutional Court characterized *the Right to Self-Determination of Private Information* as "a right of the information subject to control when and where and how far his/her personal information is disclosed and used," which means "a right of the information subject to decide the disclosure and use of his/her personal information by him/herself." Moreover, the Court stated that "the personal information that shall be protected within *the Right to Self-Determination of Private Information* are the matters that characterize one's independent personality, such as one's physical figure, belief, personal position, status, etc., and are not limited to the information in one's private or personal area but rather cover personal information formed in public areas, or even previously disclose information." The Court also held that "all the actions like investigation, collection, storage, processing, management, etc. targeted for personal information are in principle subject to the restrictions of *the Right to Self-Determination of Private Information*."[6]

---

[5] The Supreme Court 1998. 7. 24. Sentence 96DA42789 Judgment. The main issue in this case was whether National Securities Headquarters' secret collection and management of information about citizens' activities of association and assembly constitute torts. The Supreme Court here acknowledged that the State is liable for compensating damages of plaintiffs, as their fundamental rights have been infringed by the State's tort.

[6] The Constitutional Court 2005. 5. 26. Sentence 2004HeonMa190 Judgment. In this case, the Constitutional Court stated that "as for the legal basis of the *Right to Self-Determination of Private Information*, general personality rights based on freedom of privacy and secret from the Constitution's Article 17, human worth and dignity and right to pursue happiness from the first sentence of Constitution's Article 10, or together with these Articles, and the basic free and democratic constitutional principles or principle of national sovereignty or democracy shall be considered. However, as it shall be impossible to completely embrace the substances of the *Right to Self-Determination of Private Information* into one of the fundamental rights of principles of the Constitution, it is undesirable to confine its Constitutional basis on any one or two of them, and rather it would be more reasonable to consider the *Right to Self-Determination of Private Information* as right unindicated in the Constitution which is ideologically based on the principles ahead."

Henceforward, in a case that dealt with a congressman of the National Assembly disclosing on the Internet the names of teachers who joined the teachers' union, the Supreme Court held that it is reasonable for the lower court to decide this kind of behavior infringes the teachers' "*Right to Self-Determination of Private Information* which derived from personality rights and others."[7] As the Supreme Court decided that "general personality rights or the right to privacy derived from the Constitution shall also be specified through general provisions of the Civil Law in a form of personality interests guaranteed by private law,"[8] I believe that *the Right to Self-Determination of Private Information* which form a part of personality rights also should be understood as personality rights in private law.

Most scholars tend to approve the right to personal information on the level of privat e law because disclosure and use of personal information have direct influences on persona lity manifestation and human dignity.[9]

Thus in Korea, personal information is not only approached in the aspects of property value, but also characterized as a part of personality rights and it can be appraised that the *Right to Self-Determination of Private Information* is accepted as an exclusive right that can exclude its infringement like one of absolute rights such as real rights.[10]

B. "The Personal Information Protection Act" as a General Law for Protection of Personal Information

"The Personal Information Protection Act" was established on 29 March 2011 and enforced on 30 September 2011 as a general law regarding the protection of personal information of the general public, including employee and employer.

Before this Act was established, public areas and private areas were separately regulated as to the protection of personal information.[12] "The Personal Information

---

[7] The Supreme Court 2011. 5. 24. Sentence 2001MA42430 Judgment.

[8] The Supreme Court 2011. 9. 2. Sentence 2008DA42430 Full Bench Judgment.

[9] *See* Kim Jae Hyung, *Generals of Personal Rights*, Studies on Civil Law Judgments. vol. 21. Park Young Sa (1999); Lim Gyu Cheol, *Studies on Right to Self-Determination of Private Information in Information Society.* Studies on the Constitution. vol. 8. no. 3, Korean Society of Constitutional Law (2002); Lee Sang Don and Jeong Hyeon Uk, *Motives of Information Use,* Korean Law. no. 47. Legal Research Institute of Korean University (2006); Lee In Ho, *Understanding Personal Information Protection Act as Second-Age Privacy Protection Law*, The Civil Law. no. 8. Foundation of Supporting Civil Law Research (2009); Jeong Sang Jo and Kwon Young Joon, *Protection of Personal Information and Remedies for Damages in Civil Law*, BubJo. no. 630. Association of Judical Officers (2009), etc.

[10] Kwon Tae Sang, *Protection of Personal Information and Personal Right*, 4 Ewha L.J. 99. vol. 17 (2013). The Court also stated that "personality rights is hard to be fully recovered by remedies for damages (monetary remedy or measures of regaining reputation) once infringed and it is hard to expect effective complement for damage, so therefore, for infringement on personality rights, preliminary methods like cease and desist or prevention of infringement shall be accepted." (The Supreme Court 1996. 4. 12. Sentence 93DA40616,40621 Judgment). In other words, "right of honor as personality rights is a right with exclusiveness" and thus "it is possible to request for cease and desist or prevention of infringement to the offender." (The Supreme Court 2005. 1. 17. Sentence 2003MA1477 Judgment).

[12] The "Act on the Protection of Personal Information Maintained by Public Institutions" was applied to public sectors for the protection of personal information, whereas the "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.," the "Use and Protection of Credit Information Act," the "Act on Real Name Financial Transactions and Confidentiality," and the "Act on the Protection, Use, etc. of Location Information," etc. were applied to the private sectors.

Protection Act" was established as a general law that can be applied both on public and private sectors,[13] and so the "Act on the Protection of Personal Information Maintained by Public Institutions" has been abolished. However, other laws which were previously applied to private sectors, such as the "Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.", are still applied.[14]

1. Purpose and Scope of the Law

The purpose of the "Personal Information Protection Act" is "to prescribe matters concerning the management of personal information in order to protect rights and interests of all citizens and further realize the dignity and value of each individual by protecting personal privacy, etc. from collection, leakage, misuse and abuse of individual information."[15] Thus, this Act has its direct basis on the Constitution's Article 10 assuring human worth and dignity and the right to pursue happiness, and Article 17 assuring the right of privacy, and actualized the *Right to Self-Determination of Private Information* which the Constitutional court had explicitly approved.[16]

The Personal Information Protection Act applies to public institutions, corporate bodies, organizations, individuals, etc. regardless of their size if they process personal information.[17] It covers hand-written documents as well as electrically handled personal information within its scope of protection[18] in an attempt to resolve the blind areas of the law.[19]

2. Scope

Personal information in the Act is defined as "information that pertains to a living person, including the full name, resident, registration number, images, etc. by which the individual in question can be identified, (including information by which the individual in question cannot be identified but can be identified through simple combination with other information)."[20] As there is no specific limitation on the character, content, or form of the information in the Act, any type or form of information by which the individual in question can be identified becomes the object of the Act.[21] Thus, CCTV filmed images are included as personal information, and employees' personal information in the process of recruitment, and employment through retirement are also included as discussed below.

The term "information subject" means "a person who can be identified by the

---

[13] Due to this enactment, constitutional institutions like the Court, nonprofit organizations, enterprises, and about 3 million institutions that were outside of regulations are now presumed to be applied to the Act. (Kim Gwang Sam, *Establishment of the Personal Information Protection Act and Political Subjects*, Korean Policy Academy Spring Meeting Proceedings (2011), p.562).

[14] There is a critical opinion that Acts or subordinate statutes related to personal information protection scattered in individual laws should be abolished and rearranged, for reasons of collision and contradiction with the Personal Information Protection Act and the existence of unnecessary redundant regulations. *See* Lee Chang Beum, *The Personal Information Protection Act*, Bub Mun Sa 68-69 (2012).

[15] *See* Article 1 of the Personal Information Protection Act.

[16] The Constitutional Court 2005. 5. 26. Sentence 99HeonMa513,etc. Judgment.

[17] *See* paragraph 5 Article 2 of the Personal Information Protection Act.

[18] *See* Article 3 of the Standard Personal Information Protection Guidelines, the Ministry of Public Administration and Security. No. 2011-45 (Sep. 30, 2011) established as per Article 12 (1) of the Personal Information Protection Act.

[19] *See* the National Assembly Bills Information System Bills (No. 11087).

[20] *See* Paragraph 1 Article 2 of the Personal Information Protection Act.

[21] Lee Chang Beum, *supra* note 13 at 15.

managed information and therefore is the subject of given piece of information,"[22] and special contract relation is not required between the personal information manager and the information subject.[23] Therefore, as long as an individual is relevant to the information subject, he/she would be within the scope of protection by the Act, whether he/she is an employee or just an applicant, prospective recruit, or retiree.

According to the Act, the personal information manager, who has the duty of protecting personal information, is "a public institution, corporate body, organization, individual, etc. who manages personal information directly or via another person to administer personal information files as part of his/her duties."[24] Thus, in a case where an employer takes care of personal information to manage personal information file—an aggregate of personal information both in electrical and hand-written documents, systematically arranged or organized according to a specific rule for the purpose of readily retrieve personal information—for managing the business, he/she conforms to the personal information manager and so the Act would be applied. Therefore, in labor relations the Personal Information Protection Act is applied to the employer's protection of employees' personal information. Article 6 of the Act prescribes that "unless otherwise provided for in other Acts including the 'Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.', and the 'Use and Protection of Credit Information Act', the protection or personal information shall be governed by this Act," so the other Acts are applied when provided. However, as discussed below, because regulations in labor law areas about employees' right to privacy and personal information are very limited, the Personal Information Protection Act performs as a general law in substance.

3. Principle of Personal Information Management

According to the "Personal Information Protection Act," consent of the information subject should be obtained when collecting personal information, and only in exceptional cases prescribed by the Act is it not required. In addition, personal information can only be used for the intended purpose.[25] When obtaining consent, an information subject must be notified of the purposes for which personal information is collected and used, items of personal information to be collected, period for which personal information is held and used, etc.[26] When a personal information manager collects personal information, he/she shall collect the minimum information necessary for achieving the purpose thereof, and in such cases, the personal information manager is responsible for proving that he/she collects the minimum personal information.[27] A personal information manager shall not reject providing an information subject with goods or services on the ground that the information subject does not give consent to collect his/her personal information other than the minimum necessary information.[28]

The Act prohibits the use and restriction of personal information other than the purpose thereof when providing personal information to a third party, except for

[22] *See* Paragraph 3 Article 2 of the Personal Information Protection Act.
[23] Lee Chang Beum, *supra* note 13 at 28.
[24] *See* Paragraph 5 Article 2 of the Personal Information Protection Act.
[25] *See* Article 15 (1) of the Personal Information Protection Act.
[26] *See* Article 15 (2) of the Personal Information Protection Act.
[27] *See* Article 16 (1) of the Personal Information Protection Act.
[28] *See* Article 16 (3) of the Personal Information Protection Act.

exceptional cases such as existing special provisions in any Act, criminal investigation, judicial affairs, and so forth.[29] Compared with the collection and use of personal information, in cases where it is inevitably necessary for entering into and performing a contract with an information subject, or where it is obviously necessary for a personal information manager, the consent of the information subject is not required.[30] However, when providing personal information to a third party, consent is not an option. Therefore, requirements for providing personal information to a third party are stricter.

Requirements for use and provision of personal information beyond the purpose without consent are even stricter than collecting and using personal information or providing a third party with personal information, as abuse of personal information occurs most frequently in such situation.[31]

For sensitive information such as thought, beliefs, joining or withdrawal from a labor union or political party, a political opinion, etc., and unique identifying information or resident registration number, it provides separate restriction, prohibiting management except for cases where he/she obtains consent of the information subject or where special provisions exist in any other Act.[32] Moreover, considering the frequency of managing personal information through entrustment of affairs, specific provisions are provided for on restrictions on management of personal information following entrustment of affairs.[33] When personal information becomes unnecessary as its holding period expires, its management purpose is achieved and by any other ground, information shall be destroyed without delay unless the personal information must be preserved pursuant to any other Act or subordinate statute.[34]

No one shall install and operate image data processing equipment such as CCTV in a public space except in the cases for public purposes provided in the Act.[35] An information subject has "a right to receive information concerning the management of personal information," "a right to choose and decide whether he/she consents to the management of his/her personal information, the scope of consent, and related matters," "a right to verify whether personal information is managed and to request an inspection of personal information (including issuance of a certified copy; hereinafter the same shall apply)," "a right to request the suspension, correction, deletion and destruction of personal information," and "a right to receive relief from damage caused by the management of personal information according to prompt and fair procedures," regarding the management of his/her personal information.[36]

4. Relief Procedure in Case of Violation

The "Personal Information Protection Act" provides distinctive regulations compared to the "Civil Law" for the purpose of simplifying the procedure of relief in case of infringement.

First, concerning the compensation for damage, if an information subject suffers loss

---

[29] *See* Article 17 (2) of the Personal Information Protection Act.
[30] *See* Paragraph 4 and 6 Article 15 (1) of the Personal Information Protection Act.
[31] *See* Article 18 of the Personal Information Protection Act.
[32] *See* Article 23 through 24-2 of the Personal Information Protection Act.
[33] *See* Article 26 of the Personal Information Protection Act.
[34] *See* Article 21 of the Personal Information Protection Act.
[35] *See* Article 25 of the Personal Information Protection Act.
[36] *See* Article 4 of the Personal Information Protection Act.

as a personal information manager has violated this Act, he/she may claim for loss to the personal information manager. In such cases, the personal information manager cannot be exempted from responsibility unless he/she proves that he/she has performed such act neither intentionally nor by negligence.[37] Therefore, in a claim for damages pursuant to the "Personal Information Protection Act," burden of proof for intention or negligence lies with the defense personal information manager, whether it is on the part of tort or breach of contract—that is, the burden of proof is shifted.[38] Also, in a case where a personal information manager entrusts a third party with the management affairs of personal information, the Act prescribes that the trustee shall be deemed an employee of a personal information manager, when liability to pay compensation arises as a trustee violates the Act in the course of managing personal information in connection with the entrusted affairs,[39] which enables the victim to hold the personal information manager who entrusted the affairs responsible for employer's liability for damages (Article 756 of the Civil law).[40]

Second, when many subjects of information suffer the same or similar types of loss or infringement of their rights, they may apply for mediation of a dispute collectively to the Dispute Mediation Committee,[41] and if the problem is not solved, certain consumer organizations or non-profit, non-governmental organizations may institute an action requesting for the prohibition or suspension of an infringement on rights (hereinafter referred to as "class action") in a court.[42]

C. The Protection of Communications Secrets Act

The purpose of the Protection of Communications Secrets Act is to protect the secrets of communications.[43] According to this Act, no person shall censor any mail, wiretap any telecommunications,[44] or record or listen to conversations between others.[45] Any person who illegally tapped or attempted to tap communications are to be punished.[46] The term "tapping" here means "acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or interfering with their transmission and reception."[47] Therefore, an employer is forbidden to surveil telecommunications such as telephone or e-mail without the consent of the employee. Also, Article 4 of the Act prescribes that "the contents of

---

[37] *See* Article 39 (1) of the Personal Information Protection Act, Article 32 of the Act On Promotion Of Information and Communications Network Utilization and Information Protection, Etc., *See also* Article 43 (1) of the Use and Protection of Credit Information Act.

[38] Lim Gyu Cheol, *21th Century Personal Information Policies and Acts*, Book For You, 272 (2013).

[39] *See* Article 26 (6) of the Personal Information Protection Act.

[40] *See* Article 786 of the Civil Law. *See* also Kwon Tae Sang, *supra* note 10 at 104.

[41] *See* Article 49 of the Personal Information Protection Act.

[42] *See* Article 50 through 57 of the Personal Information Protection Act.

[43] *See* Article 1 of the Protection of Communications Secrets Act.

[44] The term "telecommnuications" means transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fiber cable or other electromagnetic system, including telephone, e-mail, membership information service, facsimile and radio paging. *See* paragraph 3 Article 2 of the Protection of Communications Secrets Act.

[45] *See* Article 3 of the Protection of Communications Secrets Act.

[46] *See* Articles 16 through 18 of the Protection of Communications Secrets Act.

[47] *See* Paragraph 7 of Article 2 of the Protection of Communications Secrets Act.

communication acquired or recorded through illegal wiretapping shall not be admitted as evidence in a trial or disciplinary procedure." Thus when an employee agreed with an employer's surveillance of telephone or e-mail, it is not considered as illegal wiretapping and thus can be used as evidence in disciplinary procedure; even if there was no consent from the employee, information other than communication collected by electronic surveillance and tapping conversation are not in the scope of regulation—which is the limit of the Act.[48] Furthermore, there are limits for the protection of employees' personal information in a way that this Act cannot be applied to personal information other than 'communication' and 'conversation'.[49]

D. The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

This Act, purposed to protect personal information of people using information and communications services,[50] prescribes restriction on use of personal information collected by providers of information and communications services,[51] protective measures for personal information,[52] prohibition on disclosure of personal information,[53] etc. However, as this Act basically regulates collecting, processing, etc. of personal information between the providers of information and communications and the users, it is not be applied on collecting and processing of personal information between the employer—who is not a provider of information and communications—and the employee. Article 49 states, "No one shall mutilate another person's information processed, stored, or transmitted through an information and communications network, nor shall infringe, misappropriate, or divulge another person's secret" and have penal provisions for violation.[54] Thus, there are possibilities of applying this Act on mutilation, infringement of employees' personal information which are processed, stored, or transmitted through an information and communications network by the employer. Nevertheless, as Article 49 of this Act covers "another person's" information or secret, the protection of employees' personal information would have its limits, for it is often difficult to distinguish whether the information collected by electronic surveillance in workplaces are possessed by the employer or the employee.[55]

---

[48] Kim Kyung Hwa, *Plans to Protect Employee's Rights from Labor Restrictions using Electronic Surveillance System*, Korea Law vol. 51, The Korean University Academy of Law (2007), p.135

[49] *See* The National Human Rights Commission of Korea Decision, 'RECOMMENDATION FOR IMPROVEMENT OF LAW AND SYSTEM FOR PROTECTION OF EMPLOYEE'S PERSONAL RIGHTS IN WORKPLACE ELECTRONIC SURVEILLANCE' (Dec. 11, 2007).

[50] *See* Article 1 of The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

[51] *See* Article 24 of The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

[52] *See* Article 28 of The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

[53] *See* Article 28-2 of The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

[54] *See* Article 71 of The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

[55] Kim Kyung Hwa, *supra* note 47 at 136.

E. The Act on the Protection, Use, etc. of Location Information

The purpose of this Act is to protect privacy from the leakage, abuse and misuse of location information.[56] According to this Act, no one shall collect, use, or provide the location information of an individual or mobile object without the consent of the individual or the owner of the mobile object.[57] Also, in cases where a location information provider, etc. intends to collect personal location information, the consent of the subjects of personal location information must be obtained in advance.[58] So it is prohibited to track and regulate the location of an employee, who is the subject of personal location information, without his/her consent inside and outside of the workplace. However, this Act has limitations, for it is impossible to regulate electronic surveillance issues on personal information other than location information.

F. The National Human Rights Commission Act

The National Human Rights Commission Act is purposed to contribute to the embodiment of human dignity and worth as well as to safeguard the basic principles of democracy, by ensuring that inviolable fundamental human rights of all individuals are protected and the standards of human rights are improved.[59] For this purpose, the National Human Rights Commission was established to deal with affairs for the protection and improvement of human rights.[60] The National Human Rights Commission perform various duties like investigation and remedy with respect to human rights violations,[61] and if deemed necessary to protect and improve human rights, it may recommend related entities to improve or rectify specific policies and practices or present opinions thereon.[62] Moreover, it may initiate an investigation by petition or *ex officio* in cases where human rights have been violated or a discriminatory act has been committed,[63] and may recommend implementation of remedial measures.[64]

The National Human Rights Commission has approved the "Information and Communication Technologies (ICTs) and Human Rights" as a sort of human right, and has defined it as "a fundamental right to use digitalized information freely without discrimination and desecration of human worth and dignity in accordance with the process of collecting, processing, distributing and utilizing digitalized information and the value of the information obtained through the process thereof," and up holds the right to information privacy, freedom of expression on the Internet, right to access information, and right to enjoy information and culture as its specific contents.[65] For this reason, the National Human Rights Commission took care of various types of civil rights affairs dealing with information privacy violations, such as monitoring, tapping, collection and

---

[56] *See* Article 1 of The Act on the Protection, Use, etc. of Location Information.
[57] *See* Paragraph 1 of the Article 15 of The Act on the Protection, Use, etc. of Location Information.
[58] *See* Articles 18 and 19 of The Act on the Protection, Use, etc. of Location Information.
[59] *See* Article 1 of The National Human Rights Commission Act.
[60] *See* Article 3 of The National Human Rights Commission Act.
[61] *See* Article 19 of The National Human Rights Commission Act.
[62] *See* Article 25 of The National Human Rights Commission Act.
[63] *See* Article 30 of The National Human Rights Commission Act.
[64] *See* Article 44 of The National Human Rights Commission Act.
[65] The National Human Rights Commission of Korea, INFORMATION HUMAN RIGHTS REPORT 11-16 (2013).

leakage of personal information.[66]

The National Human Rights Commission has the right to investigate on a vast range the privacy of employees and infringement on personal information, but its recommendations do not have legal binding effects, but rather must be accepted voluntarily by the parties involved.

G. The Labor Legislations

There are no direct provisions in the current Labor Related Acts which regulate electronic surveillance or protection of employees' personal information. The Labor Standards Act prescribes prohibition of forced labor,[67] free use of recess hours,[68] and private life of workers lodging in a dormitory annexed to the business or workplace[69]; but it is only limited to confined objects or indirect restrictions, which is not enough for the protection of employees' privacy and personal information. "The Trade Union and Labor Relations Adjustment Act" prohibits "Dismissal or unfavorable treatment of a worker on grounds that he has joined or intends to join a trade union, or have attempted to organize a trade union, or have performed any other lawful act for the operation of a trade union"[70] and "Domination of or interference in the organization or operation of a trade union by workers"[71] as unfair labor practices. Therefore, it can be regulated to monitor union members or collect information of labor union through electronic surveillance, but it is difficult to say employees' privacy and personal information is within its scope of protection directly. Moreover, the "Employment Agency Act" prescribes "no person who has participated or is participating in job placement services, business providing vocational information, business recruiting workers or labor supply business shall divulge any confidential information concerning workers or employers which comes to his/her knowledge in the course of conducting his/her duties,"[72] which gives duty of confidentiality of an employees' collected personal information to the employer.

Besides, according to the "Act on the Promotion of Workers' Participation and Cooperation," "installation of surveillance equipment for workers within a workplace" is prescribed as one of the matters requiring consultation by a labor-employer committee,[73] and any workers' member may demand material related to the consultation and the relevant employer shall sincerely comply with such demand.[74] Although it is the only provision related to surveillance of employees in the labor legislations, in respect that it is possible

---

[66] To see the present conditions of civil complaints about monitoring, tagging, circulation of information, etc. that has been reported to the National Human Rights Commission of Korea, 31 cases in 2001, 315 cases in 2002, 1,518 cases in 2004, 1,69 cases in 2006, 3,261 cases in 2008, 4,359 cases in 2010, 5,559 cases in 2012, which shows gradual increase. In 2012, more than 30% of civil complaints were reported compared to 2011, that is, 3.7 times more than 2004, 2.5 times more than 2006. Especially, from 2001 through end of 2012, complaints about CCTV were reported up to 6,120 cases taking largest proportion (20%) of civil complaints in accordance with Information Privacy. (*ibid* note 1 at 141).

[67] *See* Article 7 of The Labor Standards Act.

[68] *See* Article 54 (2) of The Labor Standards Act.

[69] *See* Article 98 (1) of The Labor Standards Act.

[70] *See* Paragraph 1 of Article 81 of The Trade Union and Labor Relations Adjustment Act.

[71] *See* Paragraph 4 of Article 81 of The Trade Union and Labor Relations Adjustment Act

[72] *See* Article 42 of The Employment Agency Act.

[73] *See* Article 20 (1) 14 of the Act on the Promotion of Workers' Participation and Cooperation.

[74] *See* Article 14 of the Act on the Promotion of Workers' Participation and Cooperation.

for an employer to refuse the demand of an employee, provided "material which falls under the management or business secret of enterprise" or "personal information,"[75] and that it is not a matter of 'co-decision'[76], and thus it is impossible to compel employer's consultation, it is difficult to see this Act as being effective. Furthermore, the "Equal Employment Opportunity and Work-Family Balance Assistance Act" forbids discrimination on grounds of gender in recruitment and employment, and prescribes that "in recruiting or employing female workers, no employer shall exhibit or demand physical conditions, such as appearances, height, weight, etc., and unmarried conditions not required for performing the relevant duties, or any other conditions determined by Ordinance of the Ministry of Employment and Labor,"[77] which protects personal information of female workers to some extent. Nevertheless, it has limitations for it is only applied to female workers.

III. Relation between Employer's Interest, and Employees' Privacy and Personal Information

A. Legal Basis for Employee Privacy and Protection of Personal Information and Necessity of Balancing

As discussed above, current labor legislation has limits to be used as a basis for active protection of employee privacy or personal information. Thus, it would be proper to find legal basis for the protection of employees' privacy and personal information from the Personal Information Protection Act directly, and from the principal of good faith and essence of labor relations or incidental duty of employment contract indirectly, on a background of personality rights and the *Right to Self-Determination of Private Information* guaranteed by the Constitution.

The principal of good faith means "an abstract standard that prohibit the parties of legal relations from exercising a right or performing a duty against fairness or faith, in behalf of other parties' interest."[78] As the Supreme Court proposes, since there is no reason the principal of good faith is not applied in labor relations, employers take responsibility of considering the benefits of employees' privacy and personal information in the course of employment.

Considering that the employee provides his/her labor or service combined with his/her whole personality, protection of employee's right to privacy and personal information has special meanings. As long as the labor relations exist, the employer has the right to direct and control whether the employee is fully executing the duty of performance, or properly using the employer's property suitably while in the workplace; and this process may involve monitoring and surveillance of the employee, and collection and use of the employee's personal information. Different from the surveillance of equipment or property of the company, however, surveillance of the employee or collection and use of the employee's personal information always has the underlying possibility of intrusion on the employee's right to privacy and the *Right to Self-Determination of Private Information*.

First, to discuss surveillance by the employer related to the employee's right to

[75] *See* Article 14 of the Act on the Promotion of Workers' Participation and Cooperation.
[76] *See* Article 21 of the Act on the Promotion of Workers' Participation and Cooperation.
[77] *See* Article 7 of the Equal Employment Opportunity and Work-Family Balance Assistance Act.
[78] The Supreme Court 2013. 12. 18. Sentence 2012DA89399 Full Bench Judgment.

privacy, the employer can generally monitor employees or their working processes through direction and supervision, *on and off or intermittently*. Also, for the employee's part, it is naturally accepted and approved that his/her work shall *sometimes* be monitored and surveilled by the employer due to the characteristics of labor relations, so the employee's right to privacy can be restricted in this process by some degree. Nevertheless, when the surveillance is conducted not in a momentary or intermittent way but rather in a continuous or periodical way, infringement on privacy may occur *continuously and periodically* as well, especially when equipment such as the telephone, Internet, CCTV, etc. are used under regular and systematic restrictions. To acknowledge regular or systematic infringement on privacy by surveillance by the employers as lawful, it would be necessary to balance between the legitimate interest of the employer and the infringement of an employee's privacy. In balancing between conflicting interests, it should be taken into account that the protection of the employee's right to privacy has two meanings: the employee's defense rights from the infringement on privacy by the employer (i.e., negative aspect of employee's right to privacy), and the duty of the employer to protect the employee's right to privacy (i.e., positive aspect of employee's rights to privacy). Even though specific legitimacy of infringement on an employee's privacy by the employer's surveillance can be individually judged depending on the type of surveillance under all circumstances, whether the employer is following related provisions or principle of proportionality including legitimacy of purpose, reasonableness of means, and appropriateness of surveillance methods is a required consideration.

In connection with the protection of an employee's personal information, employees' *Right to Self-Determination of Private Information* has special meanings in labor relations. In recruitment or during the employment, the employer normally collects a considerable amount of an employee's personal information. Particularly, when monitoring an employee with technology, personal information is collected no matter what the employee intended. In such situation, leaving the employee as the object of information instead of the information subject contravenes one's human dignity. That is because if the collection and processing of personal information becomes usual and institutional, the employee would become to feel that every aspect of his/her life is being traced, which would gradually lead to the forfeiture of his/her human identity. In this sense, the employee's *Right to Self-Determination of Private Information* is significant not only because it is a measure of defense from indiscriminate collection of personal information by the employer, but also because it is the starting point of actively securing human identity in labor relations. Employee's *Right to Self-Determination of Private Information* has, however, limits like any other rights. In cases where the employer's freedom of enterprise and significant interests are evident, employee's *Right to Self-Determination of Private Information* can be limited based on the principle of proportionality. In determining the legitimacy of proportioning, purpose and contents of the "Personal Information Protection Act" should be taken into account, as well as the basic principles of proportionality.

B. Requirements for the Employer to Collect and Monitor the Employee's Personal Information

The Personal Information Protection Act prescribes that in cases where it is necessary for a personal information manager to realize his/her legitimate interests and this obviously takes precedence over the rights of an information subject, a personal

information manager may collect personal information and use it for the intended purpose of collection without the consent of an information subject.[79] In such cases, this shall be limited to cases where such information is substantially relevant to the personal information manager's legitimate interests and reasonable scope is not exceeded.[80] According to Article 15 of the Act, in cases where the employee's personal information is substantially relevant to the employer's legitimate interests and reasonable scope is not exceeded, the employee's personal information may be collected without his/her consent as long as it is necessary for the employer to realize his/her legitimate interests and this obviously takes precedence over the *Right to Self-Determination of Private Information* of the employee. In other words, to legitimately collect personal information without the employee's consent, the following requirements must be met: first, the employee's personal information shall be substantially relevant to the employer's legitimate interests; second, the collection shall not exceed reasonable scope; third, the employer shall realize his/her legitimate interests; and fourth, this interest shall obviously take precedence over the employee's *Right to Self-Determination of Private Information*.[81] It would be possible to analogize these requirements to surveillance on employees.

First, collecting an employee's personal information has to have substantial relevance to the employer's reasonable interests. Installing CCTV or monitoring the employee's Internet use for the purpose of preventing leakage of business secrets or robbery, or of safety supervision, investigations or inspections for tracking the leaker of business secrets would be considered as substantially relevant to the employer's legitimate interests.[82] The employer's legitimate interests may sometimes have legal basis such as securing safety and health in the workplace, or have contractual basis like monitoring propriety of performance.

"Substantial relevance" is defined as cases where the employer's 'legitimate interests' cannot be protected or are very difficult to be protected without processing such personal information.[83] For example, when an employer sustains loss due to robbery in the workplace and a certain employee is suspected of the crime, but there are no other proper means to secure evidence, collecting information from covert surveillance through CCTV would be allowed.[84]

Second, collecting employee's personal information should not exceed its reasonable scope. For example, installing personal CCTV to surveil every employee for the purpose of monitoring propriety of performance would be regarded as exceeding reasonable scope and would be restricted. To decide whether it is within reasonable scope or not, the purpose of personal information collection or monitoring should be considered together. To be recognized as 'reasonable scope', it has to be on its minimum extent necessary for

---

[79] *See* paragraph 6 of Article 15 (1) of the Personal Information Protection Act.

[80] *See* paragraph 6 proviso of Article 15 (1) of the Personal Information Protection Act.

[81] Compared to the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Article 7 (f) of EU which requires only "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed," the requirement of the Personal Information Protection Act is much stricter.

[82] *See* Ministry of Public Administration and Security, Explanation of the Personal Information Protection Act 82 (2011.12).

[83] Lee Chang Beum, *supra* note 13 at 133.

[84] Ha Gyeong Hyo, *"Legal Problems on Introduction of New Labor Surveillance System"*, 18 Labor Law 125, Korean Society of Labor Law (2004).

achieving the purpose of monitoring or collecting. Moreover, the means of collecting personal information or monitoring should be considered for the determination of whether it is within 'reasonable scope'. If there is no reasonableness of its means—like installing hidden cameras for prevention of robbery—personal information collected by such means cannot be recognized as 'reasonable'. Therefore, the methods or degree of the means has to be considered as well.

Third, collecting an employee's personal information or surveillance on an employee has to be necessary for realizing the employer's legitimate interests. Whether the actions of collecting employee information, etc., are necessary or not should be decided by considering the specific purposes of collecting the information or the equipment for monitoring.[85] Installing an electronic time recorder to manage an employee's absence, or installing CCTV to prevent robbery by employees or others would be considered as "necessary."

Fourth, the employer's legitimate interests should obviously take precedence over the *Right to Self-Determination of Private Information* or privacy of the employee. For example, measures such as installing CCTV in a staff lounge for prevention of robbery, monitoring every employee e-mail,[86] or installing monitoring system for breakdowns of Internet access for prevention of the leaking of business secrets[87] would infringe an employee's privacy and personal information excessively, and thus be forbidden.

On the other hand, even if the employee consents to the collection of personal information or surveillance, such would not be permitted if the contents violate essential aspects of human dignity. For example, installing CCTV in bathrooms or fitting rooms for safety would not be admitted even if the employee consented, according to the "Personal Information Protection Act."

IV. Personal Information Protection in Recruitment Process

A. Consent from Applicant

When an employer receives applications from applicants, he/she is able to collect vast personal information from the applicants. According to the Personal Information Protection Act, a personal information manager has to obtain the consent of an information subject in cases of collecting personal information.[88] However, in cases where it is inevitably necessary for entering into and performing a contract with an information subject, the consent is not needed.[89]

In the Personal Information Protection Act, it prescribes that the Minister of Security and Public Administration may establish 'Standard Personal Information Protection Guidelines'[90] concerning standards for managing personal information, etc., and encourage the personal information managers to comply therewith.[91] According to the 'Standard

---

[85] *Ibid* at 114.
[86] Lee Chang Beum, *supra* note 13 at 132.
[87] The Ministry of Public Administration and Security, *supra* note 81 at 83.
[88] *See* paragraph 1 of Article 15 (1) of the Personal Information Protection Act.
[89] *See* paragraph 4 of Article 15 (1) of the Personal Information Protection Act.
[90] The 'Standard Personal Information Protection Guidelines' are only recommendations; they are not legally binding.
[91] *See* Article 12 (1) of the Personal Information Protection Act.

Personal Information Protection Guidelines',[92] "cases where it is inevitably necessary for entering into and performing a contract with an information subject" means "cases where it is impossible or remarkably difficult to enter into a contract with the information subject and perform the duties of contract without collecting and managing personal information," and in the *Explanation of the Personal Information Protection Act* by the Ministry of Security and Public Administration, it interprets, "'entering into a contract' includes 'preparation for the contract'."[93] According to this interpretation, it is basically possible to collect and use an applicant's application before concluding a contract without consent of the applicant.[94]

After concluding an employment contract, it is possible for the employer to collect and use the employee's personal information without his/her consent, for it is "inevitable for performing a contract."[95]

B. Scope of Collectable Personal Information

Regardless of an applicant's consent,[96] when an employer collects an applicant's personal information, he/she shall collect the minimum information necessary for achieving the purpose thereof. In such cases, the employer is responsible for proving that he/she has collected the minimum personal information.[97]

In accordance with this provision, the scope of personal information which the employer is capable of collecting from applicants on recruitment would be limited to the minimum information necessary. Information capable of confirming an applicant's identity (e.g., name, date of birth), information necessary for contacting the applicant (e.g., telephone number, address, etc.), and information needed to evaluate the performance abilities of the applicant (e.g., level of education, grade, certificate, etc.) would fit into this range. The scope of collectable personal information would vary depending on the characteristics and content of the job. When a certain level of education and certification is necessary for the work, related information can be collected; but when such information is not needed—such as, for example, in work requiring manual labor—it would not be regarded as minimum information.

Information irrelevant to recruitment, such as family members' occupation, marriage

---

[92] *See* Notification of the Ministry of Public Administration and Security (Sep. 30, 2011) (No.2011-45).

[93] *See* Ministry of the Security and Public Administration, *Explanation of the Personal Information Protection Act,* 2011.12, at 79.

[94] *See* The Ministry of Public Administration and Security and the Ministry of Employment and Labor, GUIDELINES FOR PERSONAL INFORMATION – PERSONNEL, LABOR. 25 (Aug. 2012).

[95] *See* The Ministry of Public Administration and Security, EXPLANATION OF THE PERSONAL INFORMATION PROTECTION ACT, 80 (Dec. 2011).

[96] On the Ministry of Public Administration and Security EXPLANATION OF ACT OR SUBORDINATE STATUTE, ENFORCEMENT DECREE AND DIRECTIVE OF THE PERSONAL INFORMATION PROTECTION ACT. (Dec. 2011), it states that when collecting personal information by the applicant's consent the principle of minimum collection does not apply and it only applies when there is no consent (88), which is inappropriate. That is because Article 16 (1) of the Personal Information Protection Act prescribes that even in cases "where it is inevitably necessary for entering into and performing a contract (paragraph 4 Article 15(1))" the minimum information necessary for achieving the purpose shall be collected, and employer, who is the personal information manager, has the right to decide recruitment which makes it meaningless for the applicants to give their consent and makes it more necessary to apply the principle of minimum collection.

[97] *See* Article 16 (1) of the Personal Information Protection Act.

status, family status, physical conditions, hobbies, financial status, etc., are not allowed to be collected. Furthermore, collection of personal information for determination of terms or conditions of employment in concluding an employment contract should be construed as not permitted on the ground that such would violate the principle of minimum collection.

According to the Personal Information Protection Act, the personal information manager basically shall not manage any information on the thought, beliefs, joining or withdrawal from a labor union or political party, political opinion, health, sexual life, etc., of an applicant, nor the genetic information or information of criminal record referred to as 'sensitive information', and 'unique identifying information' which refers to identifying information uniquely assigned to each individual to tell him/her from others, such as resident registration number, passport number, driving license number, foreign registration number, except for in cases where an information subject is notified of the matters referred to in the Act and his/her separate consent is obtained in addition to his/her consent to the management of general personal information, and where any Act or subordinate statute requires or permits the management of sensitive information and unique identifying information.[98] Thus, to collect information referred to as 'sensitive information' or 'unique identifying information', the employee's separate consent is required; yet even when the consent is obtained, collection of information irrelevant to the performance of duties is restricted, for such is not necessary minimum information. Even before the enactment of the Personal Information Protection Act, the Supreme Court restricted management of information, for "collecting and demanding information about certain teacher's joining or withdrawal from a labor union, or information about specific labor union violate teacher's *Right to Self-Determination of Private Information*, or teachers' and labor unions' right to organize."[99]

Besides, it is reasonable to construe that it is forbidden to collect information based on discrimination, because the equal protection clause in the Constitution and labor legislation such as "Labor Standards Act"[100] prohibit discrimination in labor relations.[101]

---

[98] *See* Article 23 and 24 of the Personal Information Protection Act, and Article 18 and 19 of the Enforcement Decree of same Act.

[99] The Supreme Court 2011. 5. 24. Sentence 2011MA319 Judgment. In accordance with this case, the member of the National Assembly who disclosed the list of names of the members joining the teachers' union in spite of the objection of the members and the court's decision, and press and other members of the assembly who carried out such information were accused of compensation from 8,193 members. The Seoul District Court sentenced them to pay a total of 1.6 billion Won (approx. 1.6 million USD) for these actions have infringed on the right to self-determination of private information and the right to organize guaranteed by the Constitution. (Seoul Central District Court 2013. 9. 4. Sentence 2011GAHAP124405 Judgment.)

[100] Article 6 of the Labor Standards Act prescribes that "An employer shall neither discriminate against workers on the basis of gender, nor take discriminatory treatment in relation to terms and conditions of employment on the ground of nationality, religion, or social status." Article 5 (2) of the Employment Promotion and Vocational Rehabilitation of Disabled Persons Act prescribes, "Employers shall not discriminate against any worker in personnel management, including employment, promotion, transfer, education, and training, merely on the ground that the relevant worker is a disabled person." Article 4-2 (1) of the Act On Prohibition of Age Discrimination in Employment and Elderly Employment Promotion prescribes, "Employers shall not discriminate against any of their workers or any person who wishes to work for them, on the grounds of age without justifiable grounds in the following areas (Recruitment and Employment)."

[101] Bang Jun Sik, *Legal Judgment of Employee's Personal Information and Privacy Protection*, 31 Hanyang Law. Academy of Hanyang Law. 307 (2010); Lim Gyu Cheol, *General Consideration of Management of Employee's Personal Information In the Personal Information Protection Act*, 45 Labor Law, Korean Society of Labor Law 353 (2013); Yu Gak Geun, *International Trends about Employee's Personal Information*

In particular, in the "Equal Employment Opportunity and Work-Family Balance Assistance Act," it prescribes that no employer shall discriminate on grounds of gender in recruitment or employment of workers; likewise, in recruiting or employing female workers, no employer shall exhibit or demand physical or marital conditions not required for performing the relevant duties, or any other conditions determined by Ordinance of the Ministry of Employment and Labor.[102] So the employer is not allowed to demand information about height, weight, marital status, etc. when recruiting female employees.

V. Protection of Personal Information and Privacy in Employment

A. Collection and Use of Personal Information by Employer in the Process of Employment

As discussed above, on the process of entering into employment contract or performing the contract, it is possible to collect and use the employee's personal information without his/her consent. That is because it is relevant to cases "where it is inevitably necessary for entering into and performing a contract."[103] Therefore, it is possible to collect and use personal information related to making decisions of working conditions, personnel appointments, education and training, and welfare without the employee's consent. Nevertheless, it is interpreted that when disclosing through bulletin board or other means the facts about personnel appointments or unfavorable dispositions (such as disciplinary action or dismissal), the consent of the employee is needed in advance, for it pertains to the provision of personal information to a third party.[104] This is because such information is not inevitably necessary for entering into and performing a contract.

Although information on 'health' falls under a category of 'sensitive information' which requires separate consent,[105] as seen above, information about health examination conducted by the "Occupational Safety and Health Act" do not require consent, for it applies to the cases "where there exist special provisions in any Act or it is inevitable to fulfill an obligation imposed by or under any Act and subordinate statute."[106] On the other hand, information about health examination not conducted by any Act or subordinate statute corresponds to 'sensitive information'.

Meanwhile, to provide a third party with the personal information of an employee, consent of an employee has to be obtained.[107] When providing information to a third party, even if it is inevitably necessary for entering into and performing a contract, the employee's consent is mandatory. So in cases where the employer provides personnel

---

Protection, 13 Collection of Labor Law Theories. Korean Society of Comparative Labor Law. 45-46 (2008).

[102] *See* Article 7 of the Equal Employment Opportunity And Work-Family Balance Assistance Act. In accordance with the statement, there are critical comments that this Article only applies to female employees and by demanding picture in documents the employer may know the prohibited information. *See* Lim Gyu Cheol, *supra* note 100 at 353.

[103] *See* paragraph 4 Article 15 of the Personal Information Protection Act.

[104] Same opinion; *See* the Ministry of Public Administration and Security and the Ministry of Employment and Labor, GUIDELINES FOR PERSONAL INFORMATION – PERSONNEL, LABOR. 32 (Aug. 2012).

[105] *See* Article 23 of the Personal Information Protection Act.

[106] *See* paragraph 2 Article 15 (1) of the Personal Information Protection Act.

[107] *See* paragraph 1 Article 17 (1) of the Personal Information Protection Act.

information for interchange of personnel between affiliated companies, and provides customers with personnel information, consent of the employee is required.

When obtaining consent to provide a third party with information, an employer must notify the employee of the following: "the recipient of personal information," "purposes for which the recipient of personal information uses such information," "items of personal information to provide," "period for which the recipient of personal information holds and uses such information," and "the fact that an information subject has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent."[108] The time of consent is not legislated, but considering the purpose of consent, it should be obtained clearly and in advance.[109]

B. Protection of Personal Information and Privacy Related to Electronic Surveillance System

1. Installation of CCTV, etc. in the Workplace

In the Personal Information Protection Act, the term "image data processing equipment" is defined as equipment that is permanently installed in a certain space to photograph the images, etc. of a person or an object, or to transmit such images via a wired or wireless network, such as closed-circuit television (CCTV), and network camera,[110] and also restricts installation and operation of image data processing equipment in public spaces.[111] In here, according to the Court, defining "public space" as apartment complex or paths in campus which are connected to the road where barrier is not installed, or even installed, no special installation exists, but opened for everyone to pass through by car,[112] and the Court seeing "public space" as a public parking lot that is not for a specific mall, operates without a keeper or charge where unspecified people can frequently use,[113] it can be defined as public place such as road, park, plaza or place allowed for unspecified people to use or enter.[114] On paragraph 11 Article 2 of the 'Standard Guidelines for Personal Information Protection', notification of Security and Public Administration, 'public space' is prescribed as "places like park, road, subway, mall, parking lot, etc., where an information subject has no limitations on approaching and passing through."

Thus, the Personal Information Protection Act's Article 25 would not be applied to CCTV which is installed inside a workplace, since it is not a public space. On the other

---

[108] *See* Article 17 (2) of the Personal Information Protection Act.

[109] *See* Article 22 of the Personal Information Protection Act prescribes the methods of Consent. *See also* Lee Chang Bum, *supra* note 13 at 150.

[110] *See* paragraph 7 of Article 2 of the Personal Information Protection Act and Article 3 of the Enforcement Decree of same Act.

[111] *See* Article 25 of the Personal Information Protection Act.

[112] The Supreme Court 2006. 1. 13. Sentence 2005DO6986 Judgment.

[113] The Supreme Court 2005. 9. 1. Sentence 2011DO319 Judgment.

[114] However, there are critical comments that as the intention of Article 25 of the Personal Information Protection Act is to permit collection of personal image information without consent of the information subject in situations where it is difficult to obtain each subject's consent, and in return, to recover information subject's right to self-determine infringed personal information through opening public hearing, expert's advice, installation of guideboard, etc., it is reasonable to see 'public space' as places where so many people come and go that it is impossible to obtain consent from every one of them, and not only places allowed for 'unspecified people' to enter but also for 'restricted unspecified people' should be seen as public space. *See* Lee Chang Bum, *supra* note 13 at 236.

hand, as the images filmed by CCTV are in the range of personal information, in accordance with the Personal Information Protection Act, the general principle of collection and use of personal information would be applied.[115] Ultimately, for installation of CCTV, the consent of every person being monitored is required. Only in cases where paragraphs 2 through 6 of Article 15 (1) of the Personal Information Protection Act are applied, installation and operation thereof without advance consent would be regarded as lawful. Here, whether exceptional reasons may apply or not, especially in cases "where it is necessary for a personal information manager to realize his/her legitimate interests and this obviously takes precedence over the rights of an information subject" may come into question, as already discussed above. Furthermore, as collection of personal information in accordance with the Personal Information Protection Act has to be limited to the minimum information necessary for achieving the purpose, necessary minimum range in specific cases may come into question as well. It is necessary to balance between legitimate interests of the employee and employer.

In balancing, we need to 1) determine the object of surveillance, 2) consider the specific purpose of the monitoring system, and 3) evaluate the importance of all circumstances of interests.[116] When decision is made through this process that the employer's controlling interest is larger, the employee has the duty to accept installation and operation of surveillance system, but only in minimum range necessary for achieving the purpose. The employer also has the duty of notifying the employee in advance about installation of surveillance system and the surveillance.[117]

2. Surveillance by Monitoring Internet and E-mail

"The Protection of Communications Secrets Act" provides that "No person shall censor any mail, wiretap any telecommunications, provide the communication confirmation data, record or listen to conversations between others that are not made public, without following the provisions under this Act, the Criminal Procedure Act or the Military Court Act."[118] The Act also prescribes penalties for any person who has censored any mail, wiretapped any telecommunications or recorded or eavesdropped on any conversations between other individuals in violation of the provisions.[119] Here, the term "telecommunications" means transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fiber cable or other electromagnetic system, including telephone, e-mail, membership information service, facsimile and radio paging,[120] and the term "tapping" means acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the

---

[115] *See* Lee Chang Bum, *supra* note 13 at 234.

[116] Kim In Jae, *Legal Restrictions for Electronic Labor Surveillance*, Issues of 2006 Labor Law. Korean Labor Research Academy. 266 (2007); Ha Gyeong Hyo, *supra* note 83 at 114-115.

[117] Ha Gyeong Hyo, *supra* note 83 at 116; However, Kim Tae Jeong, *Meaning of Employee's Privacy and the Range of Protection*, 22 Labor Law. Korean Society of Labor Law. 21(2006) explains the following as detailed substances of proportionality: i) existence of reasonable reasons for surveillance, ii) surveillance uniformly done in a way that least infringes on employee's privacy, iii) consultation being made in accordance with the enforcement of surveillance, iv) clearly notify of principles of surveillance in employment rules, etc., and inform him/her in advance when carrying out the surveillance.

[118] *See* Article 3 of the Protection of Communications Secrets Act.

[119] *See* Article 16 of the Protection of Communications Secrets Act.

[120] *See* Article 2 (1) of the Protection of Communications Secrets Act.

consent of the party concerned or interfering with their transmission and reception.[121]

According to this Act, monitoring internet and e-mail would be relevant to tapping telecommunications. In a recent case where the Supreme Court judged whether 'packet tapping' is permitted by this Act, it held that "transmission or reception through Internet network correspond to the term 'telecommunications' in paragraph 3 Article 2 of the Protection of Communications Secrets Act, so acquiring or recording the contents of packet which is in a form of flowing electronic signal by procuring it in the middle through Internet network, in other words 'packet tapping', would be permitted if requirements are met as stated in Article 5 (1) of the same Act unless there are other special situations, and it would not be seen differently only for the concern of tapping unrelated third party's communications due to the characteristics of packet tapping."[122] In other words, the court has seen 'packet tapping' as one of the communication-restricting measures of the Protection of Communications Secrets Act.[123] Therefore, an employer monitoring Internet and e-mail without the consent of the employee would indicate violation of the Protection of Communications Secrets Act and would be restricted.

The remaining problem is whether monitoring Internet use and e-mail would be permitted if the employer obtained consent from employees. As a limit of electronic labor surveillance, actions that bring essential infringement of human dignity would be prohibited. Furthermore, a balancing test may be applied to these circumstances. Several purposes can be listed, such as monitoring Internet use and e-mail, prevention of the leaking of business secrets, detection or prevention of criminal offense, engagement in work, and improvement in performance of employees. There is a possibility of essential infringement on personality rights of an employee when monitoring Internet use and e-mail, as it is possible for the employer to surveil the entire history of an employee's Internet surfing, contents of e-mails, and even contents of text messanging in real time, as discussed above. Even when the employee gives his/her consent, such monitoring may be regarded as illegal as it is against the principle of minimum collection of information necessary, and essentially infringes on the human rights of the employee, because by only monitoring e-mails that are appraised as specifically necessary for the employer's controlling interests are permissible.

3. Methods of Consent as Requirement for Adopting Electronic Surveillance System

The Personal Information Protection Act requires consent of each information subject as a principle of collecting personal information. As methods of obtaining consent, it is clearly understood that respective matters requiring consent must be classified and the information subject of such matters must be notified, and consent be obtained respectively to such matters (Article 22). For more specific methods, consent can be obtained through the form of signature and seal delivered in person, by mail or by fax; through oral consent by telephone; or display through Internet homepage or by e-mail, etc.[124] Furthermore in the Protection of Communications Secrets Act, consent indicates individual consent like

[121] *See* paragraph 7 of Article 2 of the Protection of Communications Secrets Act.
[122] The Supreme Court 2012. 10. 11. Sentence 2011DO319 Judgment.
[123] It means censorship of mail or any wiretapping of (Article 3 (2) of the Protection of the Communications and Secrets Act).
[124] *See* Article 17 (1) of the Enforcement Decree of the Personal Information Protection Act.

censorship and tapping, etc.; there is no special regulation for the methods of consent. However, it is preferred to have documentary consent to easily prove the employee's consent in cases where problems arise concerning the lawfulness of collecting information by means of surveillance.[125]

When restrictions for the methods of consent in the Personal Information Protection Act do not apply, as in CCTV in the workplace, the problem of validity of consent may occur in cases where the employer uses a way of putting in a consent clause in the employment contract *en bloc*, or by inserting a reference clause such as 'Others refer to employment provisions in related regulations' for the purpose of securing consent altogether. Considering the imbalance in power between the employer and employee in labor relations, it is doubtful that the employee's consent is genuine in individual labor relations;, rather, it is more likely that the employee is compelled to give consent due to his/her inferiority.[126] Therefore, genuine intent of the employee should be determined by considering specific aspects of documentary consent; inserting only a reference clause in an employment contract without notifying the employee of the detailed contents of the labor surveillance would not be recognized as valid.[127]

C. Issues of Recognizing Employee's Right to Demand Inspection, Correction, Deletion of Personal Information

An information subject may request a personal information manager to allow him/her to inspect his/her personal information. When a personal information manager has received an inspection request, he/she shall ensure that an information subject can inspect the relevant personal information within 10 days, unless there exist justifiable grounds making it impractical to inspect such information within the specified period.[128] The objects of information that can be requested for inspection include not only information that the information subject provided in hand, but also information collected from a third party or open source (e.g., reputation of information subject, articles on the Internet, in the newspaper, a magazine, etc.), information produced by personal information manager (e.g., credit evaluation, personnel evaluation, transactional information, etc.), and so forth.[129] An information subject who has inspected his/her personal information may request a personal information manager to correct or delete his/her personal information, and the personal information manager shall investigate the personal information in question without delay, take necessary measures, such as correction, deletion, etc., and notify the information subject of the result, unless other Acts and subordinate statutes stipulate special procedures.[130]Furthermore, in the sense that the information subject shall be able to

[125] Ha Gyeong Hyo, *supra* note 83 at 119.
[126] Park Gue Cheon, *Employer's Problems of Surveillance and Restriction on Employee*, 29 Legal Law Studies. Seoul National University Legal Law Research Institute. 261 (Sep. 2010).
[127] Ha Gyeong Hyo, *supra* note 83 at 119.
[128] *See* Article 35 of the Personal Information Protection Act. However, in cases where it is forbidden by provisions, where there are possibilities of illegal infringement on other person's personal security, property, etc., the personal information manager should notify such cases and limit or deny the request of inspection. For details on requesting inspection, *see* Article 41 and 42 of the Enforcement Decree of the Personal Information Protection Act.
[129] Lee Chang Bum, *supra* note 13 at 326.
[130] *See* Article 36 of the Personal Information Protection Act. However, when in other provisions such personal information is listed as object of collection, deletion may not be requested. For details on requesting

withdraw his/her consent even after allowing management of information, the information subject may request a personal information manager to suspend the management of his/her personal information, and the personal information manager in receipt of such request shall immediately suspend the management of the personal information completely or partially.[131]

In accordance with the above provisions of the Personal Information Protection Act, the employee can inspect personal information which the employer collects and possesses, and request for correction when there is an error or for deletion when the holding period expires. Thus, the employee has the right to inspect his/her personnel information depending on the Personal Information Protection Act's Article 35 (2). Requesting for inspection of base materials for assessment of performance or salary, however, would be restricted or denied when such disclosure may encroach on the interests of the employer or other employees.[132]

D. Issues of Personal Information of Retired Employees after the Employment Relations

When personal information becomes unnecessary as its holding period expires, its management purpose is achieved and by any other ground, a personal information manager shall destroy the personal information without delay, unless the personal information must be preserved pursuant to any other Act or subordinate statute.[133] When employment relations are terminated, granted that the purpose of collecting an employee's personal information may cease to exist, the employer shall destroy personal information of the retired employee.[134] However, Article 39 of the Labor Standards Act prescribes that whenever an employer is requested by a worker to issue a certificate specifying the term of employment, kinds of work performed, positions taken, wages received, and other necessary information, he/she shall immediately prepare and deliver a certificate based on facts, even after the retirement of the worker. Article 42 of the same Act prescribes that an employer shall, for three years, preserve a register of workers and other important documents related to labor contracts as prescribed by Presidential Decree, and there, the Enforcement Decree of Labor Standards Act's Article 22 lists employment contracts, wage ledgers, documents pertaining to the basis for the determination, payment method and calculation of wages, documents pertaining to employment, dismissal, or retirement, documents pertaining to promotion or demotion, documents pertaining to leaves of absence, etc. as "important documents related to an employment contract as prescribed by

---

deletion, *see* Article 43 of the Enforcement Decree of the Personal Information Protection Act.

[131] *See* Article 37 of the Personal Information Protection Act. However, when differently stated in any Act, existing possibility of illegal infringement on other person's personal security, property, etc., or public institutions performance may be bothered, etc., cessation may not be requested. For details on requesting cessation, *see* Article 44 of the Enforcement Decree of the Personal Information Protection Act

[132] *See* The Ministry of Public Administration and Security and the Ministry of Employment and Labor, GUIDELINES FOR PERSONAL INFORMATION – PERSONNEL, LABOR. 36 (Aug. 2012).

[133] *See* Article 21 of the Personal Information Protection Act. When destroying personal information, it should be done in a manner that cannot be restored or regenerated, and when storing the information relevant to the exceptional cases, those personal information or personal information file should be separately stored and managed. *See* Article 21 of the Personal Information Protection Act.

[134] Kwon Oh Seong, *Brief Study of Protection of Employee's Personal Information*, vol. 12 no. 3 Hong Ik Law, University of HongIk Legal Institute. 183 (2011).

Presidential Decree." Therefore, for the purpose of complying with the demands of the Labor Standards Act, an employer may store certain scope of personal information of a retired employee. If stored information of a retired employee within the range of such purpose is too vast, intent of the Personal Information Protection Act may be neglected.[135]

Meanwhile, the problem of an employer providing a prospective employer with personal information of a retired employee when requested may come into question. Prudent handling is demanded in such cases where an applicant's personal information is collected indirectly without his/her recognition, for there are strong chances of unforeseen infringements.[136] According to the Personal Information Protection Act, a personal information manager shall obtain the consent of an information subject in principle when providing a third party with the personal information of an information subject.[137] In this sense, if a former employer tries to provide another employer with personal information of a retired employee, consent of the retired employee is needed. When obtaining consent about third party provision, he/she shall notify an information subject of a recipient of personal information, purposes for which a recipient of personal information uses such information, items of personal information to provide, period for which a recipient of personal information holds and uses such information, the fact that an information subject has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent.[138]

Furthermore, when a personal information manager manages personal information collected from a person other than the information subject, he/she shall immediately notify the information subject of the collection source of personal information, purpose for which personal information is managed, the fact that the information subject has the right to request the suspension of managing the information, if so requested by the information subject.[139] Therefore, prospective employer who collected information about a retired employee from a former employer must notify him/her of collection source of personal information, purpose for which personal information is managed, etc. upon his/her request.

VI. Conclusion

In our information society, social economic system establishes and develops on the basis of production of added value by collecting and processing information in accordance with rapid advancements in information and communication technologies. Thanks to such technological advancements, personal information can be massively collected and easily used, making greater the possibility of information infringement or misuse. In such a society, the protection of a person's personal information is greatly needed. In Korea, movements to establish a unified and systemized personal information protection act began

[135] Such Labor Standards Act and the Enforcement Decree of Labor Standards Act seems to be prescribed without considering the importance of personal information, and therefore, it should certainly be revised in a way to limit the scope of information in reference with the purposes of issuing certificates and duty of the employer to conserve documents.

[136] Kwon Oh Seong, *supra* note 133 at 175-176.

[137] *See* Article 17 (1) of the Personal Information Protection Act.

[138] *See* Article 17 (2) of the Personal Information Protection Act.

[139] *See* Article 20 of the Personal Information Protection Act. Nevertheless, in cases where providing notification could harm any third party's life or physical safety, or infringe national safety, etc., the personal information manager may deny the notification. *See* Article 20 of the Personal Information Protection Act.

to rise as early as 2003. After eight years of discussion, the Personal Information Protection Act was established in 2011. From a formal point of view, this Act changed historically the separated personal information protection system (that is, the binary system of the public and private sectors) into an integrated information management system. From a contents point of view, considering the differences in the various kinds of personal information protect regulations in Korea, the Act oriented toward meeting the global standards stage by stage. It is obvious that the Act provided a turning point for the protection of personal information in Korea. However, some concerns have been raised in the course of enactment of the Act (for example, there are no preventive enforcement functions but more *ex-post* systems, no independent supervisory authority exists, etc.).[140] With the recent case of vast data leakage of credit card companies in Korea,[141] such concerns and problems have been realized.

From the perspective of labor law, it is too early to properly analyze the effects of the newly-established Personal Information Protection Act in the labor market, or whether it effectively protects employee's privacy and personal information. Nevertheless, from a normative view, the Personal Information Protection Act can be judged as incomplete legislation which does not reflect the distinct characteristics of employment relations. This is because the Act, which tried to find the balance point between 'the value of protection' and 'the value of utility' of personal information on the basis of the neutral concept of information subject and personal information manager, does not consider the imbalance in power, as well as the imbalance in information between the employer and the employee (who works under subordinate relations). For example, the consent of the information subject that works as a fundamental device for protection of personal information in this Act cannot be expected to effectively function in labor relations. Moreover, with regard to the distinct characteristics of labor, infringement of an employee's privacy or personal information is already internationalized and structuralized in labor relations. It is almost impossible to expect that an employee's privacy or personal information can be fully protected by an Act that lacks such consideration.

To make the employee's *Right to Self-Determination of Private Information* effectively respected in workplaces, independent labor legislation should be established, which includes substantive restrictions and preventive measures focusing on the unlimited accumulation and misuse of an employee's personal information collected by an employer's electronic surveillance as well as labor unions' and employees' right of collective participation in dealing with personal information. When these requirements are met, labor, in the era of information society, will be able to work in a workplace rather than in a panopticon.

---

[140] Seong Nak In, et al., *Legislation Assessment of the Personal Information Protection Act System,* Korea Legislation Research Institute. 935 et seq. (2008).

[141] According to the *Financial Supervisory Service*, on 11 December 2013, the personal data of 130, 000 and 34,000 customers of Korea Standard Charter Bank and Korea Citi Bank, respectively, had been illegally leaked to loan solicitors. In addition and especially, on 8 January 2014, the personal information including name, telephone number, card number, etc. on 104 million credit cards of three large credit card companies had been illegally leaked to loan solicitors. *See* Announcement of the Financial Supervisory Service, 19 January 2014.