COESOFTLAW・DISCUSSION・PAPER・SERIES

COESOFTLAW-2004-9

Worker's Personal Information and Privacy Protection and Japan's Employment System

Takashi Araki
Professor of Law, Dr., The University of Tokyo,
Graduate Schools for Law and Politics.

10/2004

Workers' Personal Information and Privacy Protection and Japan's Employment System

By Takashi Araki

1 Introduction

Until very recently, Japanese labor law paid little attention to protection of workers' personal information and workers' privacy. This might be because information technology developments and a rapid diffusion of internet and e-mail use which make people recognize the need for personal information protection are rather recent phenomena. In the author's opinion, however, it seems more closely related to the characteristics of the Japanese employment system where employers have been allowed or even expected to collect personal information of workers as much as possible in order to properly manage their personnel. Here "properly" means not only for the benefit of employers but also workers. When the Japanese employers implement any measure of personnel management such as worker transfers, they have been supposed to carefully consider workers' personal situations including those of workers' family members. In order to do so, Japanese employers have to collect a lot of personal information of workers.

This article, therefore, first discusses the relationship between the Japanese employment system and workers' personal information and privacy issues. Second, this article will give an overview of the legal framework for personal information protection. Third, medical information and employment relations will be examined. Fourth, e-mail monitoring and workers privacy will be discussed.

2 Japanese Employment System and Personal Information

Employment relations in Japan have been characterized by the long-term employment practice commonly known as "lifetime employment." The typical model of the practice is as follows. A new recruit enters a company immediately following graduation and enjoys secure and stable employment until he reaches the mandatory retirement age, which is usually the age of 60. He receives systematic in-house education and training and experiences various types of work under a periodical transfer program. This high level of employment security coupled with the flexible deployment of personnel leads Japanese employers to collect as much personal information as possible regarding each worker. Workers take it for granted that conveying personal information to their employer would afford the employer the opportunity to take their personal situation into consideration when strategies are considered.

The following three phases of the Japanese employment system will illustrate such relationship between little awareness of regulations regarding workers' personal information and the employment system.

2.1 Employers' freedom to investigate applicants' beliefs and creed at the time of hiring

First, the prevalence of the long-term employment relationship under which the employers' right to dismiss is significantly restricted because of the courts' severe scrutiny of the abusive exercise of

rights and the corresponding high level of security regular workers enjoy, has made employers cautious in selecting job seekers not only as to whether the person can provide normal service but also as to whether he/she is suitable to continue long-term relationship as a member of the corporate community until mandatory retirement age. Such consideration leads the Supreme Court decision on the *Mitsubishi Jushi* case[1] to interpret the employer's wide freedom of hiring to include a refusal to hire based upon thoughts and creed, and also a wide freedom to investigate the individual's beliefs and creed. In the *Mitsubishi Jushi* case, the employer refused to hire a person as a regular worker upon completion of the probationary period[2] on the grounds that he made a false statement with regard to his experience with political activities on his personal statement which was submitted to the company at the time of the recruiting examination, and that the making of the false statement itself disqualified him as a managerial candidate.

The court faced the question as to whether the company's refusal runs counter to the Constitutional provisions of equality under the law (Constitution Art. 14[3]) and freedom of thought and conscience (Constitution Art. 19[4]), as well as the prohibition of discrimination in working conditions on account of creed under the Labor Standards Law (LSL Art. 3[5]). The Supreme Court held that the human rights provisions of the Constitution do not apply directly to relations between private individuals and that Article 3 of the Labor Standards Law refers to the post-hiring working conditions but does not regulate hiring itself. Emphasizing that the Constitution guarantees companies' freedom of doing business and of executing contracts guaranteed by Articles 22 and 29 of the Constitution, the Supreme Court ruled that even if a company refused to employ a person with a certain belief or creed on account of such characteristics, the failure to hire cannot be automatically condemned as illegal.

In connection with the freedom of hiring, this case raised the question of whether a company was permitted to investigate an applicant's beliefs or creed in the hiring process. The Supreme Court held the view that it was not illegal to do so because even the very refusal to hire on account of beliefs or creed was itself not unlawful.

In the light of the Supreme Court stressing that "employment relations in a company…call for mutual trust in the context of a continuous human relationship, and it is all the more so in a society like Japan where lifetime employment is an established fact of life…,"[6] long-term employment practices seem to influence the Court's interpretation of the employer's freedom to hire. Under the long-term employment practices, a regular worker, once employed, cannot be dismissed without a compelling

---

[1] The *Mitsubishi Jushi* case, Supreme Court, Grand Bench (December 12, 1973), 27 *Minshu* 1536.
[2] It is common practice for Japanese employers to set a probationary period for regular workers at the initial stage of employment.
[3] Constitution Art. 14 reads "All of the people are equal under the law and there shall be no discrimination in political, economic or social relations because of race creed, sex, social status or family origin."
[4] Constitution Art. 19 reads "Freedom of thought and conscience shall not be violated."
[5] LSL Art 3 reads "An employer shall not engage in discriminatory treatment with respect to wages, working hours or other working conditions by reason of the nationality, creed or social status of any worker."

reason, such as serious misconduct. Therefore, the Court perhaps thought employers should be free to investigate a candidate's personality *before* concluding a regular employment contract, to ascertain whether they can start such long-term relations.

2.2 The Duty to Care Worker's Personal Situation in Ordering Transfers

The long-term employment practice in Japan has been supported and sustained by the flexible deployment of personnel. Employment security begets the rigidity in adjusting the size of work force. To compensate for such a lack of "numerical (external) flexibility," the Japanese employers have introduced "functional (internal) flexibility" by the flexible transfers of workers within a company.[7]

Japanese employers are understood to reserve a right to order transfer of workers entailing a change of workplace and/or functions. According to the established case law[8], employers must consider inconveniences for the worker caused by the transfer order. For instance, when an employer disregards the worker's or his family member's illness or other inconveniences, such transfer order may well be regarded as an abuse of the right to order a transfer. A typical case would be one in which an order was issued for the transfer of a worker from the company's main office in Tokyo to its branch office in Hiroshima. At that time, three members of the worker's family were ill[9] and depended on his care and income. There was no difficulty in transferring another worker as a substitute. The court held that the transfer order was an abuse of rights[10].

Thus, employers endeavor to collect personal information of workers including that of their family members.

On the part of workers, they have benefited by providing personal information to their employer because, by so doing, workers have been able to expect employer's proper attention to the workers personal situation and avoid inconvenient transfer orders.

2.3 Employers' Duty to Care for Workers' Health and Safety (*Anzen Hairyo Gimu*)

Employers have been supposed to collect medical information of workers in order to perform the obligation required by the Industrial Health and Safety Law (IHSL). Under the IHSL, employers are obliged to do annual checkups on their workers. As a result, medical information of workers is accumulated by the employers.

Employers also owe the duty to care for workers' health and safety.[11] In order to perform the

---

[6] The *Mitsubishi Jushi* case, Supreme Court (December 12, 1973), 27 *Minshu* 1536.

[7] As to the comparative analysis of flexibility of the Japanese employment system, see Takashi Araki, "Accommodating Terms and Conditions of Employment to Changing Circumstances: A Comparative Analysis of Quantitative and Qualitative Flexibility in the United States, Germany and Japan", in Chris Engels & Manfred Weiss (eds.), *Labour Law And Industrial Relations At The Turn Of The Century* 509 (Kluwer, 1998).

[8] Toa Paint case,

[9] His older brother had epilepsy, his younger sister suffered from valvular disease of the heart, and his mother had high blood pressure.

[10] The *Nihon Denki* case, Tokyo District Court (Aug. 31, 1968) 19 *Romin-shu* 1111. For a similar ruling, see the *Hokkaido Coca Cola Bottling* case, Sapporo District Court (July 23, 1997) 723 *Rodo Hanre*i 62.

[11] The duty to care for workers' health and safety was first recognized as an obligation arising from contract by the Supreme Court decision in 1975. The *Jieitai Sharyo Seibi Kojo* case, Supreme Court

duty, employers are required to collect detailed medical information on workers. Recently, the so-called *KAROSHI* (death from overworking) problems and mental health of workers attracted people's attention. Accordingly, the employers' duty to care for workers' health and safety is understood to be heavier than ever. To prevent a workers' death from brain and heart diseases triggered by overworking and work-related mental diseases, employers are required to consider the individual worker's health conditions and stresses and to properly adjust work load and work environment.

2.4 Changes in the employment system and the emergence of workers' privacy protection

As illustrated above, the Japanese employment system allows and encourages employers to collect workers' personal information. Various measures taken in the Japanese employment system presuppose that employers possess ample personal information with respect to each worker.

However, the circumstances concerning workers' personal information are drastically changing. First, the long-term employment practice is waning, lateral mobility has increased and unemployment rate is more than doubled (from 2.1% in 1990 to 5.3% in 2003). This may call into question the rationale of the *Mitsubishi Jushi* decision which emphasized lifetime employment. Second, in accordance with the development of discrimination law such as the strengthened Equal Employment Opportunity Law, the emerging new concepts of discrimination such as age discrimination, discrimination against the disabled, and recognition of the so-called "sensitive data" related to race, political views, religion, beliefs and creed, union membership, health, and so forth which are prone to cause discriminatory treatment, employers freedom to collect and investigate personal information started to be re-examined. Third, developments in case law and legal theory concerning the protection of personal rights and privacy also require the re-consideration of the traditional employment system relying on employers' paternalistic intervention in employment relations utilizing accumulated personal information of workers.

Before discussing the impact of these changes on privacy issues, the developments in information technology and the legislative response in order to protect personal information should be mentioned.

3 Personal Information Protection in Employment Relations

The developments in information technology and the rapid diffusion of the Internet and e-mail usage[12] give rise to new legal issues and require new measures to protect workers privacy and to balance workers' and employers' interests at the workplace.

(February 25, 1975) 29 *Minshu* 143.1975.

[12] As of December 2000, 47 million people utilize the Internet - 74% more than in December 1999. In the workplace, more than 70% of Japanese companies have introduced e-mail, Internet and LAN systems. Among white-collar regular workers, about 95% of them use personal computers at workplace and 90% of them can be connected to networks. Ministry of Health, Labor and Welfare, "Research Report on the Impact of IT Revolution on Employment in Japan" (April 26, 2001) <http://www.mhlw.go.jp/houdou/0104/h0426-2.html> (in Japanese).

3.1 Personal Information Protection in Labor Market Regulation

3.1.1 Protection of Job Seekers' Personal Information

In accordance with the increased interests in privacy protection, the 1999 revision of the Employment Security Law (ESL) introduced regulations on personal information and secrets. Public employment security offices are required to collect, keep and utilize a job seeker's personal information[13] within a limit of being necessary to perform their functions (ESL, Art. 5-4). Furthermore, a duty is imposed to workers and ex-workers of fee-charging placement agencies to keep individual's secret obtained in the course of performing their functions (ESL, Art. 51 Para. 1). A violation of this duty is sanctioned by fines up to 300,000 yen (ESL, Art. 66, No. 9). Workers and ex-workers of public employment security offices, fee-charging and non-fee-charging placement agencies also owe a duty not to disclose personal information obtained in relation to their business though there is no criminal sanction for its violation (ESL, Art. 51 Para. 2, 51-2).

3.1.2 Protection of Dispatch Workers' Personal Information

In the late 1990s, leakage and dissemination of personal information of dispatch workers made the headlines and the necessity of legal regulations on personal information was evident. Accordingly the 1999 revision of the Worker Dispatching Law (WDL) introduced provisions requiring proper administration of personal information and confidential information.

As one of the requirements to obtain a permit for registration type worker dispatching, an agency must have taken necessary measures to properly administer personal information[14] and to keep dispatch workers' secrets confidential (WDL, Art. 7 Para. 1 No. 3).

As for personal information, a dispatching agency is required to collect, keep and utilize it within a limit of being necessary for business purposes (WDL, Art. 24-3). Accordingly, the administration of personal information is added to the duty of the responsible worker designated by the dispatching agency (WDL, Art. 36 No. 4). Client companies often request photos of dispatch workers or require an interview prior to concluding a dispatch contract with the dispatching agency. Since complaints have been made that they select dispatch workers for their looks and other non-performance related reasons, the 1999 revision of the WDL creates a duty of a client company to endeavor not to engage in such actions for the purpose of identifying dispatch workers (WDL, Art. 26 Para. 7).

As for dispatch workers' secret information, the 1999 revision of the WDL has established a duty on a dispatching agency, its proxy, and its workers not to reveal secrets obtained in the course of performing its functions. The same applies to a person who ceases to be a dispatching agency, its proxy, and its worker (WDL, Art. 24-4).

---

[13] ESL Art. 4 No. 9 defines "personal information" as "information which concerns individuals and enables to identify an individual by itself or by collating with other information."

[14] Alike in the ESL, personal information in the WDL is defined as "information which concerns individuals and enables to identify an individual by itself or by collating with other information" (Art. 7 Para. 1 No. 3).

3.2 Code of Practice of Workers' Personal Data Protection (CPWPDP)

On December 20, 2000, the Study Group on Workers' Personal Data Protection chaired by Prof. Yasuo Suwa publicized the "Code of Practice of Workers' Personal Data Protection" (hereinafter "CPWPDP"). The CPWPDP is not legally binding but encourages employers to establish rules concerning workers' personal data protection modeled on the CPWPDP.

3.2.1Principles concerning Personal Data Treatments

The CPWPDP declares the following general principles of personal data treatment.

First, the CPWPDP declares the general principles of personal data processing, such as: legal and fair processing within the limits directly related to employment; processing within the original purpose of collecting by competent workers; duty of confidentiality of the persons engaged in the personal data processing, etc.

Second, the CPWPDP establishes rules concerning the collection of personal data: namely, personal data should in principle be collected directly from the person himself. Data collected exceeding the collection purpose must not be used. The CPWPDP also prohibits collection of certain categories of data: 1) information related to race, ethnicity, social status, family origin, legal domicile, and birth place, as well as thought, creed and belief; 2) union membership or information of union activities; and 3) medical personal data.

Third, personal data must be kept within the limits of the original purpose of collection and be kept accurate and updated.

Fourth, personal data must be utilized and transferred within the limits of the purpose of collection.

Fifth, certain methods of information collection are prohibited: polygraphs, HIV tests, or genetic tests must not be used. For personality tests, alcohol tests, and drug tests, the individual's explicit consent is required. To implement monitoring by using video cameras or computers, employers should give notice of the reason, time and method of monitoring in advance except for the cases where special legal provisions allowing such monitoring exist or there are sufficient reasons to believe that a crime or other serious unfair act is committed (see 3.3.2).

3.2.2 Principles concerning Self Data Disclosure

The CPWPDP also requires employers to provide workers with information on their own personal data periodically. When the worker who finds his personal data is incorrect requests the correction or deletion of the data, the employer must accept such requests within a reasonable period.

3.2.3 Roles of Labor Unions

The CPWPDP requires an employer to notify, and to consult if necessary, the labor union concerning the introduction of automatic processing system or monitoring system. When there exits no labor union, the majority representative at the workplace shall be in the position of being notified and consulted.

3.3 The Personal Information Protection Law of 2003

In the light of information technology developments and abusive handling of personal data, it

was thought necessary to establish rules concerning the proper handling of personal information. At the same time, the need was recognized to make domestic regulations on data handling compatible with international norms. In particular, the EU directive on personal data which restricts transfer of personal data to a third country where personal data protection is not sufficient had a big impact.[15] Thus, the 2003 Personal Information Protection Law (PIPL) was enacted as the first legislation that provides comprehensive personal information protection including private sectors.[16] Corresponding to the 8 principles of the 1985 OECD guidelines,[17] the PIPL introduces various regulations for the proper treatment of personal information.

Although this Law does not specifically aim to regulate employment relations, corporations which process workers' personal data which can identify individuals such as name and birth date, and use the personal data for business including personnel management within the corporation are subject to the PIPL regulations when the number of personal data is more than 5000.[18] Therefore large corporations are required to abide by the PIPL regulations such as use limitation (Art. 16), notice of the purpose for collecting information (Art. 18), safe administration measures (Art. 20), transfer limitation to third parties (Art. 23), disclosure (Art. 25), correction (Art. 26) and suspension of data use (Art. 27), etc.

The 2003 PIPL is to be put into effect in its entirety as from April 1, 2005.

4 Medical information and employment relations

4.1 Medical Information in the Process of Hiring

As mentioned already, the Supreme Court in the *Mitsubishi Jushi* case approved of the employers' wide discretion to acquire job seekers' personal information. However, two recent lower court judgments held that the HIV test and the hepatitis B virus test conducted in the course of hiring infringed the job seekers' privacy and constituted tort.

4.1.1The *Tokyo Metropolitan Government HIV Test* Case

In the Tokyo Metropolitan Government HIV Test case[19], a plaintiff passed the examination for police service. He entered the Police School which is run by the Tokyo Metropolitan Government and was hired by the Metropolitan Police Department. The new entrants including the plaintiff had a medical checkup and blood samples were collected . The Police School did not explicitly explain what the blood test was for, and asked the Police Hospital to do the HIV antibody test. Since the result of the plaintiff's

[15] Q & A: The Personal Data Protection Bill <http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/qa-law.html>

[16] Prior to the 2003 Personal Information Protection Law, there were several laws which provided for personal information protection. However, they merely regulate administrative organs and did not cover private sectors.

[17] Eight principles are: Collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. See "OECD recommendation concerning and guidelines governing the protection of privacy and transborder flows of personal data" OECD Document C(80)58(Final), October 1, 1980.

[18] Corporations with less than 5000 personal data are exempted by the Cabinet Order No. 507 (Dec. 10, 2003) based upon PIPL. Art. 2 Para. 3 No. 4.

HIV test was positive, the plaintiff was told to have a workup without being informed of the blood test's purposes. The result of the workup confirmed the plaintiff's being HIV positive. The Police School told the plaintiff that he was HIV positive and induced him to quit the School. The Plaintiff filed a lawsuit alleging that the HIV test without obtaining the plaintiff's consent and the Police School's inducement for resignation are tortuous acts.

The Tokyo District Court held that the HIV antibody test at hiring is allowed only when there is an objective and reasonable necessity to conduct the test and when the individual concerned agreed to the test. The two HIV tests in this case were conducted not only without obtaining the plaintiff's consent but also without reasonable necessity. Therefore, the court held, the HIV tests constituted illegal acts infringing the plaintiff's privacy, and the Tokyo Metropolitan Government and the Tokyo Police Hospital were responsible for tort liability

4.1.2 The *B Kin-yu Koko [Financial Corporation] Hepatitis B Virus Test* Case

One month later from the Tokyo Metropolitan Government HIV test case, the Tokyo District Court handed down a similar judgment in the hepatitis B virus test case[20]. A plaintiff, who went through to the final stage of the recruitment selection, had the checkups two times (June 2 and 18, 1997) at the defendant's direction. Since the figures for the liver test were high, at the direction of the defendant, the plaintiff had the third health check which included the hepatitis B virus test but this fact was not explained to the plaintiff by the defendant (June 30, 1997). The result of the hepatitis B virus test, namely the plaintiff being positive, was reported to the defendant by the clinic. The defendant, without informing the plaintiff that he was hepatitis B positive, further advised the plaintiff to get a workup on his liver and the defendant's personnel accompanied the plaintiff to the workup (July 9, 1997). On July 23, 1997, the plaintiff was first informed that he was infected with the hepatitis B virus by the doctor and was shocked. On July 29, 1997, the plaintiff was told that the defendant could not agree to hire him.

Thus, the plaintiff claimed damages on the grounds that (1) the notice of declining to hire was an irrational cancellation of a tentative agreement to hire the plaintiff for the reason that he was infected with the hepatitis B virus; (2) the defendant conducted the test without obtaining the plaintiff's consent; and (3) the defendant had the plaintiff have the workup concerning hepatitis B virus without informing him of the purpose of the test.

The Tokyo District Court denied the claim based on (1) because there was no such tentative hiring agreement between the plaintiff and the defendant. However, as for the claim (2) and (3), the Court upheld the plaintiff's claim by holding as follows:

On the one hand, it was important to protect the right not to be induced into unwittingly providing samples for the collection of information on whether one is a hepatitis B virus carrier. On the other hand, employers are guaranteed the right to investigate job applicants since the freedom of hiring is guaranteed. Considering these contradicting requirements, an employer is not allowed to investigate

[19] The T*okyo Metropolitan Government* case, Tokyo District Court (May 28, 2003), 852 *Rodo Hanrei* 11.
[20] The *B Kin-yu Koko [Financial Corporation] (Hepatitis B virus test)* case, Tokyo District Court (June 20, 2003), 854 *Rodo Hanrei* 5.

the applicants concerning the hepatitis B virus unless there is a special circumstance, and even if there is a necessity for such investigation, it is required for the employer to inform the person of the purpose and necessity of the investigation and to obtain the person's consent. Therefore, the hepatitis B virus tests conducted by the defendant without explaining the purpose and necessity of the tests and without the plaintiff's consent are an illegal infringement of the plaintiff's privacy.

4.2 Medical Information in the course of Employment Relations Development

As the Japanese Industrial Health and Safety Law obliges the employer to conduct regular checkups once a year and special checkups for workers engaged in hazardous work twice a year, workers' medical information is accumulated by the employer. When work rules drawn up by an employer stipulate an obligation of the workers to have a checkup and the content is reasonable, it is understood that the workers are obliged to have such medical examination[21].

Since employers owe the duty to care for workers' health and safety, when an employer notices that a worker is suffering from some disease, it is generally permissible and sometimes obligatory for the employer to inform the worker of his disease[22]. However, in one case, an employer who informed his worker without much thought that he was infected with the HIV virus and gave him a grave shock was held liable for the socially unreasonable manner of the notification[23]. To inform third parties that the worker was infected with the HIV virus without there being a business necessity also gives rise to tort liability as an infringement of privacy.[24]

In another case where an HIV virus infected worker was dismissed, the court held that normally there is no necessity for employers to know whether a worker is infected with the HIV virus and thus employers may not collect workers' information on HIV. Therefore, the court held that to conduct an HIV antibody test infringed the right to privacy and the dismissal based upon the test was null and void.[25]

As confirmed by these cases, the employers' freedom to collect applicants' personal information, especially that which falls under the sensitive data category, is now being re-examined.

5 E-mail Monitoring and Workers' Privacy

According to the survey conducted by the Japan Institute of Labor in 2002,[26] about 90% of the surveyed companies thought that there were workers who used internet for private purposes. Although 60% replied it is not a serious problem, about 35% of surveyed companies said such private use was problematic. 35% of surveyed companies implement measures to prevent private internet use. The preventive measures were, among other things, maintaining histories of workers' web site use and e-mail use (61.3%) and the monitoring of internet use (46.2%). As confirmed by this survey, internet and e-mail monitoring by employers is not rare.

---

[21] The *Dendenkosha Obihiro-kyoku* case, Supreme Court (March 13, 1986), 34 *Minshu* 464.
[22] The *Kyowa Taxi* case, Kyoto District Court (Oct. 7, 1982) 404 *Rodo Hanrei* 72.
[23] The HIV Infected Dismissal case, Tokyo District Court (March 30, 1995) 667 *Rodo Hanrei* 14.
[24] *Ibid*.
[25] The *T Kogyo HIV Dismissal* case, Chiba District Court (June 12, 2000) 785 *Rodo Hanrei* 10.

5.1 Employers' Interests in Monitoring

Employers have several reasons for monitoring workers' e-mail and Internet access.

First, private use of e-mail or Internet, if prohibited, denotes loss of working time and a violation of the duty to engage in work faithfully. It also causes a decrease in productivity. Second, it is feared that trade secrets can be leaked through e-mails. Third, to ensure information network security, monitoring and countermeasures are required against computer viruses or hacker infiltration. Fourth, when a worker sends e-mails containing sexual harassment or discriminatory contents, it can cause a serious case of employer's liability. According to Article 715 of the Civil Code of Japan, an employer is liable for tort committed by his worker in the course of conduct of business. The notion of "conduct of business" is widely interpreted to give a generous remedy to the victim. Accordingly, several lower courts have ruled that an employer is liable under Article 715 for sexual harassment by his workers.[27] Furthermore, some recent lower-courts held that employers bear a contractual obligation to correct a hostile working environment in sexual harassment cases.[28] Article 21 of the Equal Employment Opportunity Law provides that employers shall take steps to ensure that female workers are not subject to adverse treatment or a hostile working environment resulting from sexual harassment at the workplace.

Therefore, employers seem to have good reasons to monitor workers' e-mail use and Internet access.

5.2 Privacy Protection under the Constitution and the Civil Code

On the part of workers, they have an interest to be free from employers' monitoring based upon the right to privacy. Though the Japanese laws do not have any explicit provisions protecting individuals' privacy, privacy protection can stem from the Constitution of Japan and the Civil Code.

The Constitution does not explicitly mention the right to privacy. However, Article 13 of the Constitution is understood as a comprehensive provision that guarantees fundamental human rights that are not explicitly prescribed in the Constitution.[29] Article 13 reads, "[a]ll of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental

---

[26] http://www.jil.go.jp/kokunai/statistics/web/200204/index.html

[27] For instance, in on case (the *Fukuoka Sexual Harassment* case, Fukuoka District Courts, Apr. 16, 1992, 607 *Rodo Hanrei* 6) where a supervisory worker harassed a female subordinate by spreading rumors about her sex life, the court held not only the supervisory worker but also the employer liable under the Article 715 of the Civil Code. In this case, the court further mentioned the "duty to adjust the working environment." Namely, the employer is obliged (i) to take care to prevent employment relations from developing in ways that infringe upon the worker's human dignity and diminish his or her ability to perform their job, or (ii) to cope with such an incident in an appropriate manner which will ensure that the workplace is conducive to working. The court held that the managing director had a duty to improve the work environment, but failed to do so. See Yamakawa, "Personal Rights" in the Workplace: The Emerging Law Concerning Sexual Harassment in Japan, 36-9 Japan Labor Bulletin 4 (1997).

[28] The *Kyoto sexual harassment* case, Kyoto District Court, April 10, 1997, 716 *Rodo Hanrei* 49; The *Mie sexual harassment* case, Tsu District Court, November 5, 1997, 729 *Rodo Hanrei* 54. See Ikuko Sunaoshi, "Online Rights of Japanese Workers in the Information Society" in Tadashi Hanami & Roger Blanpain, *IT Kakumei to Shokuba no Puraibashi (IT Revolution and Privacy at Workplaces)*, 238 (2001).

[29] Yasuo Hasebe, *Kenpo (The Constitution)*, 154 (2nd. 2001).

affairs." The right to privacy is generally understood as guaranteed by this Article.

Article 21 Paragraph 2 of the Constitution guarantees the secrecy of communication. Article 21 Paragraph 2 reads "[n]o censorship shall be maintained, nor shall the secrecy of any means of communication be violated."

Though the Constitutional provisions apply to the relations between the state and individuals, they do not apply directly to relationship between individual citizens, or employers and workers in the private sector. However, constitutional norms are deemed as forming "public order and good morals" or public policy and its violation is illegal (Civil Code, Art. 90). Therefore employers' acts that infringe workers' privacy or freedom of communication can be deemed as against public policy and thus illegal. Juristic acts against public policy are deemed null and void, and non-juristic acts cause tort liabilities. Tort liability is stipulated in Article 709 of the Civil Code. It provides that a person who unlawfully infringes upon another person's rights is liable for damages. According to established case law, the "rights" in this provision are interpreted as being "legally protected interests."

Accordingly, employers' monitoring of e-mail use and Internet access can be deemed as an infringement of workers' legally protected interests, or privacy. However, whether e-mail and Internet use in the workplace is protected by the right to privacy needs further examination because the personal computers and networks are provided by the employers, and are their property.

5.3 Employers' Monitoring v. Workers' Privacy

As viewed above, e-mail and Internet monitoring encompasses contradicting interests between employers' monitoring and workers' privacy. The phenomena of e-mail and the Internet are new but similar legal situations have been discussed and there are some case law developments concerning workers' privacy and human dignity at the workplace.[30]

5.3.1Inspection of personal effects

In the *Nishi-nihon Tetsudo* case, a bus driver was dismissed on the grounds that he had refused to allow his shoes to be inspected after duty. The Supreme Court set the following four requirements for the legality of such inspection: 1) there must be reasonable grounds for inspection; 2) inspections must be conducted in a generally proper manner and within appropriate limits; 3) the inspection must be implemented uniformly to the workforce as an institutionalized system; and 4) inspection must be based upon explicit grounds.[31] These four requirements are followed by the subsequent lower court decisions.[32]

In the *Kansai Denryoku* case,[33] an employer opened the worker's locker and photographed his diary without the worker's permission. The Supreme Court held that this act infringed worker's privacy and the employer was liable.[34]

---

[30] See Kiyoshi Takechi, "Netto-waaku Jidai ni okeru rodosha no kojin joho hogo (Personal information protection in the network era)", 187 *Kikan Rodoho* 35 (1998); Sunaoshi, supra note 28, 238.
[31] The Nishi-nihon Tetsedo case, Supreme Court, August 2, 1968, 22-8 Minshu 1603.
[32] See Takechi, supra note 30, 35.
[33] The *Kansai Denryoku* case, Supreme Court (September 5, 1995), 680 *Rodo Hanrei* 28.
[34] However, this case was a rather exceptional discriminatory case. In this case, plaintiffs were

5.3.2Interception and recording of workplace conversation

In the *Okayama Denki Kido* case, the employer wiretapped a workers' conversation in the workers' lounge to collect information on union activities. The court ruled that this was illegal action infringing the plaintiffs' privacy.[35]

In the *Hirosawa Jidosha Gakko [Driving School]* case,[36] the driving school installed tape recorders in the school's automobiles to record the conversations of instructors to check the quality of their lessons, without their consent. The court held that the employer should explain the reasons for recording and through in-depth consultation endeavor to obtain workers' understanding, and that recording without the free consent of workers amounts to infringement of "personal rights" or disregard for human dignity.

5.3.3CPWPDP

Case law suggests that even at the workplace and during working hours workers' privacy should be respected and that secret monitoring without obtaining workers' consent tends to be held illegal.

Considering such case law rules, the CPWPDP sets the standards as follows:

> "2-6 (4) To implement monitoring by using video cameras, computers and others (hereinafter "video monitoring"), employers should give notice in advance of the reason, period of time and the information collected by monitoring, and should pay attention not to infringe the right to personal data protection. Exceptions are allowed:
>
> i) where special statutory provisions allowing such monitoring exist, or
>
> ii) when there are sufficient reasons to believe that a crime or other serious unfair act is committed.
>
> (5) Perpetual video monitoring at the workplace is allowable only when it is necessary to secure workers' health and safety or to safeguard business property.
>
> (6) As a principle, an employer may not evaluate workers nor make a determination related to employment solely based on the results of automatic personal data processing on computers or video monitoring."

The CPWPDP 2-6 (4) does not directly regulate monitoring of e-mail use and Internet access. However, the commentary of the CPWPDP issued by the Ministry of Labor[37] suggests that e-mail monitoring should be treated under the principle of 2-6 (4) and thus it is advisable to notify workers in advance of the monitoring in company rules on e-mail use. It also advises that monitoring should be carried out only to the extent that is necessary to attain the monitoring purpose.

---

suspected of being affiliated with the Communist Party. Their superiors put them under surveillance inside and outside of the workplace, and also persuaded their peers not to communicate with them and thus isolated them at the workplace. The locker inspection was carried out in this context.

[35] The *Okayama Denki Kido* case, Okayama District Court, December 17, 1991, 606 Rodo Hanrei 50.

[36] The Hirosawa Jidosha Gakko case, Tokushima District Court, November 17, 1986, 488 Rodo Hanrei 46.

[37] *Rodosha no Kojin Joho no Hogo ni kansutu Kodo-Shishin no Kaisetus* (Commentary on the Code of Practice on Workers' Personal Data Protection) <Http://www2.mhlw.go.jp/kisya/daijin/20001220_01_d/20001220_01_d_kaisetu.html>

The commentary of the CPWPDP suggests that monitoring for the purpose of preventing private use of e-mail or Internet, leakage of business secrets, and of securing Intranet security falls under the category of "safeguarding business property." Therefore, in this case, perpetual monitoring is also allowed.

5.3.4 Recent two cases concerning legality of E-mail Monitoring

The CPWPDP is not legally binding and its proposed standards on e-mail monitoring are also not necessarily decisive and clear. Some academics propose more concrete criteria for e-mail monitoring.[38] In such situations, Tokyo District Court handed down two e-mail monitoring cases in 2003.

In *Company F Department Z* case,[39] a worker, or plaintiff, wrote an e-mail containing her critical comments on her boss, or defendant, and mistakenly sent the e-mail not to her peer husband but to the boss himself. The boss started to monitor the worker's e-mails stored in the server computer without the worker's permission and knew that the plaintiff and others were preparing to indict the defendant for sexual harassment. When the plaintiff changed passwords and the defendant could not read the plaintiff's mails, he ordered the IT division to transfer plaintiff's mails to him and continued monitoring. The plaintiff claimed that the defendant's monitoring of private mails caused tort liabilities.

The Court held that workers' private e-mail use utilizing the employer's network is allowable in the same manner as private telephone use is socially allowed within a certain reasonable limitation. When the private e-mail use remains within such limitation, it cannot be said that workers have no right at all to privacy in terms of their private e-mail use. However, the extent of privacy protection for the private use of the e-mail system provided by the company network is low compared to that in telephone use. Considering the monitoring purpose, methods and manners on the one hand and inconveniences caused to the monitored on the other, only when the monitoring exceeds the socially proper limits, does such monitoring infringe privacy.

As for this case, the court held that given the plaintiff's extreme e-mail use for private purposes and all other circumstances, the defendant's monitoring did not exceed the socially proper limits. Accordingly, the plaintiff's claim was rejected.

In the *Nikkei Quick Joho* case,[40] the plaintiff was suspected to have sent slander mails to another employee. Although there was no solid evidence that it was him, in the course of the investigation a lot of private e-mails of the plaintiff were found in the server computer. Thus, the company reprimanded the plaintiff. The plaintiff, among other things, claimed that the company's acts to print out the plaintiff's private mails and disclose them to many caused tort liabilities.

The court held that in order to maintain and restore enterprise order the company may order

[38] For instance, as a corollary to the Supreme Court's personal effects inspection rule established by the *Nishi-nihon Testuedo* case, Sunaoshi proposes four requirements: 1) there must be reasonable grounds for monitoring; 2) uniform monitoring in a less infringing manner; 3) prior consultation with labor unions; and 4) clarification of monitoring rule in work rules or other documents and giving notice to workers in question. Sunaoshi, supra note 28, 236.

[39] The *Company F Department Z case*, Tokyo District Court, December 3, 2001, 826 *Rodo Hanrei* 76.

[40] The *Nikkei Quick Joho* case, Tokyo District Court (February 26, 2002) 825 *Rodo Hanrei* 50.

necessary measures and investigate facts for disciplinary measures. However, such order and investigation must be necessary and reasonable for the smooth administration of the company and the method and manner must not amount to excessive control or restriction on human rights or freedom.

As for this case, the court held that plaintiff's sending of private mails violated the duty to concentrate on job and the manner of investigation did not exceed socially allowable limits.

It is notable that the court recognized the possibility of privacy protection for private e-mails and established a framework to balance an employer's need to monitor and the worker's interest of privacy. Concerning the result that both cases denied the infringement of privacy, however, some criticize the court as not having recognized the right to privacy to an appropriate extent.

The author thinks it would be difficult to discuss monitoring requirements in general because the nature of the requirements depends on the specific nature of issues in question. Let us take two cases: in the first a worker sues his employer, alleging monitoring without consent which infringes his privacy; in the second an employer discharges his worker on the grounds of unauthorized private use. In these two cases, the criteria for determining legality of the monitoring will not be the same. The former case depends on whether the worker's expectations for privacy is protectable or not. Therefore, if the employer explicitly declares that e-mail using the company's address and equipment will be monitored, the worker's allegation is unlikely to be approved. By contrast, in dismissal or disciplinary cases, procedural requirements can be more important and a mere declaration of monitoring policy may not be sufficient.

In any event, the two major factors which govern this issue will be: the explicit declaration of monitoring policy to avoid workers' expectations for privacy; and appropriate exercise of monitoring power in terms of the manner and extent to avoid being deemed as abuse of the right.[41] In the above quoted two cases, the employers did not explicitly prohibit private use of e-mails nor declare the monitoring policy. The Court should have paid more attention to this point.

5.4 E-mail Monitoring and Collective Labor Relations

In Japanese industrial relations, where the Trade Union Law institutes the unfair labor practice system and encourages collective bargaining, e-mail usage and e-mail monitoring cause various issues.

First of all, though it is not discussed, employers will have a duty to bargain on e-mail and internet monitoring issues because it falls under the category of mandatory bargaining subjects concerning terms and conditions of employment and other treatment of workers.[42] Thus when there is a labor union and it requests collective bargaining on monitoring, the employer cannot refuse. Refusal constitutes unfair labor practice and an administrative organ called the Labor Relations Commission will order the employer to bargain faithfully with the union.

Second, even though e-mail monitoring is generally allowed, difficult questions arise over

[41] See Tadashi Hanami, IT Kakumei to Shokuba no Kenri (IT Revolution and workers' rihgts at workplace), Hanami & Blanpain, supra note 28, iv.
[42] Kazuo Sugeno (Leo Kanowitz tr.), *Japanese Employment and Labor Law*, 563 (2002); Takashi Araki, *Labor and Employment Law in Japan*, 172 (2002).

whether the monitoring is deemed unfair labor practice intervening in the internal affairs of labor unions. Unfavorable treatment by reason of union membership is needless to say illegal and constitutes unfair labor practices.

Third, whether labor unions can request e-mail or Internet use or employers restrict their usage is also one of debatable issues of grants of conveniences to labor unions.

6 Conclusion

This article has emphasized that the development of personal information and privacy protection in Japan is triggered not only by rapid growth and developments of information technology but also by changes in the Japanese traditional employment system. Traditional Japanese labor policy has taken the position that a well-informed employer can implement well-considered personnel management. The Japanese labor law has believed in in-depth communication between the labor and management which enabled mutual understanding and cooperation.

When the value of privacy and protection of personal information surfaces, will the traditional approach totally disappear? Certainly restrictions on collecting certain personal information such as sensitive data are necessary. Employers' unrestricted freedom to investigate job seekers at the time of hiring should, as the recent cases have already suggested, be reconsidered. However, protection of personal information does not necessarily mean insulation of information flow. When proper management and utilization of information is secured, workers' personal information can still be transmitted and be utilized for agreed purposes.

Thus, how to secure proper management of information is a key issue for the Japanese employment system. In the past, in order to prevent KAROSHI or health detriment caused by overworking, employers were thought to gather more information on workers' health conditions. Recently, medical information is to be managed by a medical officer and not directly reported to the employer. Such utilization of intermediary professionals bearing strict obligation of confidentiality might be one possible device to deal with the issue of harmonizing privacy with a necessity of collecting personal information for the proper personnel management.

In traditional Japanese employment relations, regular workers have been deemed to be members of a corporate community where information sharing including personal information is not frowned upon. Protection of privacy and personal information requires us to recall that a worker is an independent individual before being a member of a corporate community. In this sense, it is certain that personal information and privacy protection is posing new challenges to the Japanese employment system.