Protection of Personal Information and Privacy in the Japanese Workplace

Ryoko Sakuraba
Kobe University

1. Introduction

A decade ago, there were no statutes specifically aimed at protecting employees' personal information and privacy in Japan. When cases involving these types of issue were brought to the courts, remedies were provided under the law of tort. The scope of coverage under such case law was far from comprehensive. This was particularly true when one considered that in certain situations companies had been allowed to question job applicants about personal matters, including political activities, during the recruitment process. Furthermore, employers have generally been encouraged to obtain and use employees' personal information, such as their health status, medical conditions and family situations under the auspices of caring for employees. Under the long term employment practice system of Japan, new-graduates hired by a company, made a career within that company until retirement, sometimes doing a variety of different jobs with additional on-the-job training. When this practice was predominant, an employer justifiably had an interest in finding out their job applicants' thoughts in order to determine whether they should be admitted into the company's community. Thus, they felt a need to obtain personal information about them so that each member of the community could live a fruitful life both at the workplace and at home.

As this paper discusses, the trend in Japan has been moving towards greater recognition of this issue.[1/2] The growing recognition of privacy and of the need to protect personal information has been extended to the workplace, particularly over the last decade.

Firstly, the scope of employees' confidential information has rapidly expanded. It is now widely known that some genes and viruses have the potential to cause diseases. For people who have these genes or are carrying these viruses, such knowledge is of course useful for medical treatment; but on the other hand, it can be a cause of discrimination in the workplace. Furthermore, the proportion of atypical workers – employees who are in the

[1] Regarding these issues, see Takashi Araki, 'Personal Information and Privacy Protection of Employees and Japan's Employment System' (2005) 8 Journal of the Japan-Netherlands Institute 167. See also, Kiyoshi Takechi, 'Netto-waaku Jidai ni okeru Rodosha no Kojin Joho Hogo' (1998) 187 Kikan Rodoho 26; Shigeya Nakajima, 'Kenko Joho no Shori Katei wo meguru Horitsu Mondai' (2005) 209 Kikan Rodoho 2; Ikuko Sunaoshi, 'Rodosha no Kenko Joho to Puraibashi' (2005) 209 Kikan Rodoho 21.

[2] Regarding the information on Japanese labour laws, see Kazuo Sugeno, *Japanese Employment and Labor Law* (Leo Kanowitz (tr), Carolina Academic Pr 2002); Takashi Araki, *Labour and Employment Law in Japan* (Japan Institute of Labor 2002); Tadashi Hanami and Fumito Komiya, *Labour Law in Japan* (Kluwer Law Intl 2011). English version of Japanese laws can be obtained on the following website. <http://www.jil.go.jp/english/laborinfo/library/Laws.htm> accessed on 20 June 2014.

workforce but not core members of company communities – has been increasing. According to the Labour Force Survey, atypical workers, including part-time workers, temporary agency workers, etc., constituted 16.4% of the labour force in 1985, but has since risen to 36.7% by 2013. This means that there are many more people who are in the workforce but outside of the company community, and thus do not expect to have their personal information collected. This is because, generally speaking, they are treated differently from the company's regular employees. For instance, while many employers reserve the right to transfer regular position employees to different places of work, they do not have the same right concerning atypical employees (e.g., part-time employees). Because of this, companies do not need to collect information about family situations of such employees.

Secondly, the collection of personal information has become effortless. Since the late 20th century, new technologies have heightened the risk of intrusion into the private sphere. Video cameras allow employers to monitor employees constantly. On the Internet, information about current and prospective employees can be easily collected. Recorders and email enable companies to monitor communications from and to their employees. Today's workplace poses a higher risk of intrusion into privacy, since employers have an interest in using surveillance and monitoring in daily management processes in order to maintain a high performing and well-ordered workforce.

Thirdly, new technologies have enabled personal information to be transmitted in volume and at a rapid rate. The first of these was the print media, which was capable of delivering information to a mass audience. This gave birth to the idea of privacy as 'the rights to be let alone' in late 19th century United States. In Japan, this concept of privacy was adopted after the introduction of this theory by academics in the 1960s.[3] In the 'Utage no Ato' case,[4] the Tokyo District Court defined privacy as 'the right [of the individuals concerned] not to have their private lives publicized in an unauthorized way'. The Court's reasoning included an examination of whether or not Yukio Mishima's novel, since it was modelled on the lives of real people, violated the privacy of the people.

The use of computers has considerably magnified the risks associated with invasions of privacy. Even if an individual piece of information about a specific person delivers little important information, combining and aggregating of individual fragments of information, may result in the exposure of important, private information about that person. The risk of information being leaked has also increased with the use of mobile and removable memory storage devices and connected networks. The proportion of businesses using the Internet in Japan reached 99.1% in 2012, while in 1998 it was only been 63.7%.[5]

In light of such a heightened risk for breaches of privacy, a number of constitutional lawyers and other academics from the field of sociology have turned their attention to the issue. The debate has focused, not only on the traditional 'right to be let alone', but also on the 'right to control one's own information' as well as 'a screening of the structure of information systems'.[6] According to these theories, in order to control one's own information, prohibitions against publication, collection or surreptitious viewing of private

[3] See Masami Ito, *Puraibashi no Kenri* (Iwanami 1963).
[4] Tokyo District Court (28 September 1964), 15-9 Kaminshu 2317.
[5] Somusho [Ministry of Internal Affairs and Communications], Tsushin Riyo Doko Chosa [Communications Usage Trend Survey] <http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html> accessed on 20 June 2014.
[6] For a summary of this discussion, see Tatsuhiko Yamamoto, 'Puraibashi no Kenri' (2012) 1412 Jurist 80.

matters are not enough. Disclosure to other persons must be also regulated; and the right to access and correct such information should be given as well. Moreover, the subject of such regulations must not be limited to confidential matters; but should extend to personally identifiable information as well. We now know that plain information may be turned into confidential information through data matching. Furthermore, considering the amount of data stored in computers, a duty to ensure proper safeguards should be imposed.

To address these risks, the Act on the Protection of Personal Information Act (PPIA 2003) was enacted to establish the duties of corporations processing personal data. According to the PPIA 2003, its purpose is to protect the rights and interests of individuals 'in view of a remarkable increase in the utilization of personal information due to the development of the advanced information and communications society' (Art. 1). This Act applies to employment relations as well.

2. Regulatory schemes for the protection of employees' personal information and privacy

A. Constitution and the law of tort

As mentioned above, the protection of personal information and privacy has been provided through case law. The legal basis of these cases had varied depending on whether the matter was public or private. In cases of public laws, where civil persons have sued national or local governments, Article 13 of the Constitution of Japan has served as the legal basis for action.[7] Article 13 stipulates that 'all 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 affairs'. On the basis of this article, the Japanese Supreme Court held that the 'freedom of private life' of citizens should be protected against the exercise of state powers.[8]

This 'freedom of private life' may include various matters. The Court held that all people shall enjoy the freedom not to have their features or figures photographed arbitrarily without their consent.[9] In another case, the constitutionality of the fingerprinting system of foreign citizens was an issue, and it was held that all people shall enjoy the freedom not to be compelled to have their fingerprints taken in an unauthorised manner.[10] In a case regarding the constitutionality of a newly instituted resident registry system, the Supreme Court held, on the basis of Article 13, that 'all of the people shall have the freedom not to have information about them disclosed or made public to third parties in an unauthorized way'.[11] This decision shows that the protection based on Article 13 extends to information that is not highly confidential in nature, such as information used in the registry system (one's name, date of birth, gender, address and a code that is assigned to each person).

Article 709 of the Civil Code has been used as the legal basis for protection in the

[7] Although the Supreme Court has not directly acknowledged the 'right of privacy' in cases involving public law relations; in effect, privacy has been protected on the basis of Article 13 of the Constitution.
[8] The Kyoto Fu Gakuren case, Supreme Court (24 December 1969), 23-12 Keishu 1625.
[9] Ibid.
[10] The Shimon Ounatsu Kyohi case, Supreme Court (15 December 1995), 49-10 Keishu 842.
[11] The Zyuki Netto case, Supreme Court (6 March 2008), 62-3 Minshu 665.

sphere of private law.[12] Article 709 prescribes that a person who has intentionally or negligently infringed upon the rights of others or the legally protected interests of others shall be liable for compensating any damages resulting from the infringement. A person liable under Article 709 must also provide compensation for damages other than property (Art. 710).[13] Privacy has been acknowledged as a 'legally protected interest' by the Supreme Court. Intrusion of privacy in employment relations has also been covered by case law. In fact, it was in a case involving an employer's incursion into the private life of an employee that the Supreme Court first used the word 'privacy'.[14] The protection afforded by case law has been extended to cover the disclosure of information, including the disclosure of prior convictions or an individual's criminal record.[15]

Case law has grown based on the above mentioned theories: 'right to control one's own information' and 'a screening of the structure of information systems'. This can be shown in a case where a list of student attendees for a lecture delivered by the President of the People's Republic China was submitted to the police by the sponsoring university. The Court held that there had been an intrusion of privacy.[16] The information in the list included student numbers, names, addresses, and phone numbers. Arguably, this information was not of a highly confidential nature. However, the Supreme Court held that it was natural for the students to expect that their information would not be disclosed to others in an unauthorised way, and that such an expectation should be protected.

What would be a crucial factor in deciding whether or not one's privacy had been unlawfully invaded? In this case, the Court reasoned that the university could easily have asked for the students' consent for the disclosure to police when students submitted the information, and held that the disclosure constituted a tort. Thus, in this case, the consent of the people concerned was crucial. On the other hand, in other instances where an individual's previous convictions were publicized by the media, the Supreme Court held that regarding privacy, when balancing the legal interests of privacy against the reasons for publishing them, and when the former is superior to the latter, this constitutes a tort.[17] To sum up the principles set force in these cases, personal information can be lawfully disclosed where any disadvantages to the victims are not so serious when compared to the necessities of the offenders, or where the consent of the victims has been obtained.[18]

---

[12] Article 13 of the Constitution cannot be a basis for legal protection in the sphere of private law. The Constitution is not directly applied to private law relations, but only indirectly. The Mitsubishi Jushi case (infra n 29).

[13] Apart from this, injunction orders have been issued in cases involving intrusion of the privacy of public figures by the press.

[14] The Kansai Denryoku case, Supreme Court (5 September 1995), 680 Rohan 28. Two employees were monitored by the employer through tailing and the inspection of their belongings.

[15] The Kyoto Shi Zenka Shokai case, Supreme Court (14 April 1981), 35-3 Minshu 620.

[16] The Waseda Daigaku Kotakumin Koen Jiken case, Supreme Court (12 September 2003), 57-8 Minshu 973.

[17] The Gyakuten case, the Supreme Court (8 February 1994), 48-2 Minshu 149; the Nagaragawa Jiken Hodo case, the Supreme Court (14 March 2003), 57-3 Minshu 229.

[18] The framework of decisions about privacy has two phases, according to the investigator of the Supreme Court in the case of the university lecture (the Waseda Daigaku Kotakumin Koen Jiken case mentioned above). In the first phase, courts should examine whether disputed acts unlawfully 'infringed upon… legally protected interests' by having invaded that person's privacy. In cases where the consent of that person is presumed, or the acts are within permissible limits, or there are public interests superior to the disadvantages of that person, such acts are not considered unlawful. Such cases include those where a friend, having known the person's participation in the lecture, told their common friend about the fact (presumed consent); or where serious criminal conviction is broadcasted by media (superior interests). Even if the acts are

B. International instruments

Japan is a member nation of both the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) forum.

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted in 1980.[19] They set forth eight principles, pursuant to which member states are recommended by the OECD Council to take measures (Para. 19). In 2004, the APEC Privacy Framework (the Framework) was adopted. The principles included in the Framework are presented in accordance with the author's own four classifications:

> (1) The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned (Para. 18). (2) According to the Framework, personal information collected should be used only to fulfil the purposes of the collection except in the following situations: where the consent of the individual has been obtained; when it is necessary to provide a service; or when it is authorised by the authority of the law (Para. 19). Personal information controllers should protect personal information with appropriate safeguards (Para. 22). When personal information is to be transferred to another person, the personal information controller should obtain the consent of the individual or exercise due diligence (Para. 26). (3) Personal information should be accurate, complete and kept up-to-date (Para. 21). Individuals should be able to obtain from the personal information controller confirmation of whether or not the controller holds personal information about them; challenge the accuracy of information relating to them and have the information rectified, completed, amended, or deleted (Para. 23). (4) A personal information controller should be accountable for complying with measures that give effect to the principles stated above (Para. 26). They should provide statements about their practices and policies (Para. 15).

A noteworthy scheme is the Cross-Border Privacy Rules System (CBPR). Under this scheme, companies can obtain certification from an 'accountability agent' after they submit answers to a self-check questionnaire concerning their compliance with the principles and after they pass the agent's examination. Agents are located in each country and each agency is itself evaluated and authorised by the Joint Oversight Panel, which is a body of APEC. Japan submitted its application for participation in the CBPR system in June 2013. If the application is accepted and an accountability agent is authorised, Japanese companies can obtain certification from such an agent.

ILO Code of Practice

considered unlawful, in the second phase, the courts should examine whether the acts were justifiable. Such cases include those where the victim's consent was obtained or could not be obtained out of necessity; or where the acts were justifiable by the authority of law (such as documents including personal information are disclosed based on a warrant). See Norihiko Sugihara, *Heisei 15-2 Saiko Saibansho Hanrei Kaisetsu Minji Hen* [Commentary on Supreme Court Decisions (Civil Cases)] (Hosokai 2006) 490-492.

[19] These Guidelines were revised in 2013. The Japanese government has set up a study group to consider revising the existing policies with regard to the use of personal data to ensure harmonization with international rules.

The above instruments do not apply only to employment relations. By contrast, a Code of Practice, 'Protection of workers' personal data' was adopted in 1996 to provide guidance on the protection of workers' personal data. It does not have binding force. However, since Japan is a member nation of the ILO, many of the principles were incorporated into the 'Code of Practice of Workers' Personal Data Protection' that was adopted by the Japanese government in 2000. The principles included in it are similar to those of the OECD Guidelines and APEC Framework, but various other matters are specially considered in the ILO Code of Practice. Reflecting the special character of employment relations, there are many regulations concerning the collection of personal data.

All personal data should, in principle, be obtained from the individual worker (6.1). Where an employer asks an employee to sign a statement authorizing the employer to obtain information about the employee, this statement must be in plain language, and be specific about the information to be obtained, its purpose, and the period of time within which the statement will be used (6.2). An employer should not collect personal data concerning a worker's sex life, political, religious or other beliefs, or criminal convictions unless it is directly relevant to an employment decision (6.5). A worker's membership in a workers' organization, or his/her involvement in trade union activities, and medical data are also matters which, in principle, must not be collected (6.6 and 6.7). If workers are monitored, they should be informed in advance, and the employer must minimize the intrusion on the workers' privacy (6.14). Regarding medical information, only conclusions relevant to a particular employment decision should be communicated to the employer (10.8). Other aspects, which need attention, are provisions concerning the involvement of employee representatives. Workers and their representatives should be kept informed of any data collection process, rules that govern that process, and their rights regarding it (5.8). The Code of Practice provides for collective rights as well. It specifically provides that before any electronic monitoring of workers' behaviour in the workplace is introduced, the workers' representatives should be informed and consulted (12.2).

C. Municipal legislation

As mentioned above, the PPIA was enacted in 2003. This Act aims to protect the rights and interests of individuals while taking into consideration the usefulness of personal information (Art. 1). The basic principle is that proper processing of personal information should be promoted under the philosophy of respecting the personalities of individuals (Art. 3).

The Act covers situations where a business operator uses a 'personal information database',[20] which is defined as 'an assembly of information systematically arranged in such a way that the specific information can be retrieved by a computer' or not by computers, but arranged in such a way that specific personal information can be easily retrieved (Art. 2, Paras. 2 and 3). Business operators which handle personal information of less than 5,000 people on any date during the last six months were excluded (Art. 2, Para. 3, No. 5, and Cabinet Order No. 507 (10 December 2003, Art. 2) for fear that the regulations would impose excessive costs on such small-and-medium-sized businesses.[21]

[20] Personal information means information about a living individual that can be used to identify the specific individual by name, date of birth, or any other description contained in such information (Art. 2, Para.1).
[21] Katsuya Uga, *Kozin Joho Hogo no Riron to Jitsumu* (Yuhikaku 2009) 71-72.

The Guidelines concerning the Protection of Personal Information for Personnel Management were issued by the Ministry of Health, Labour, and Welfare in 2012 (2012 Guidelines)[22] to amend the earlier 2004 Guidelines. The contents of the Act and Guidelines are as follows.

> First, employers must not acquire personal information by a deception or any other wrongful means (Art. 17). Second, employers must specify the purposes for which the information will be used (Art. 15). They must not process personal information beyond the parameters necessary for the fulfilment of the specified purposes, without the prior consent of the person (Art. 16). Except in cases where they have not publicly announced the purposes of utilisation of such information in advance, they must promptly notify the person of, or publicly announce, these purposes (Art. 18 Para.1). When employers acquire personal information as is written in contracts or other documents, they must clearly state the purposes for the use of such information in advance (Art. 18 Para.2).

For employers processing 'personal data', which means personal information constituting a database, the following regulations also apply (Art. 2, Para. 4):

> Employers must take necessary and appropriate measures to safeguard personal data, including the prevention of its leakage, loss, or damage (Art. 20). Such measures include giving powers of processing personal data only to certain persons and designating a person for the responsibility of controlling the personal data (2012 Guidelines). Employers must exercise necessary and appropriate supervision over their employees and/or trustees processing the personal data (Arts. 21 and 22). Employers must not provide employees' personal data to a third party without obtaining their prior consent (Art. 23). When an employer is asked by a person to stop using their personal data, and the employer do not comply with Article 16, 17 or 23, the utilisation must be suspended, or the data must be erased (Art. 27).
>
> Third, employers must endeavour to maintain personal data and ensure that it is accurate and up to date (Art. 19). They must disclose the existence of retained personal data to that person upon his/her request (Art. 25). They must also conduct corrections, additions, or deletions of personal data when they are requested to do so by the person involved (Art. 26). Reasonable charges may be collected by the entity handling the personal information (Art. 30).
>
> Fourth, employers possessing personal data must provide the following information in an accessible manner to those people. This information includes the purpose of utilisation of all retained personal data, the procedures to meet requests for disclosure, correction, deletion, etc., and the names and contacts of the persons addressing complaints about personal data, etc. (Art. 24).

Enforcement

The effectiveness of the Act is limited, considering the limitations in the coverage mentioned above, and remedies. Regarding the enforcement of the Act in the field of employment, the Minister of Health, Labour, and Welfare may request companies to explain their handling of personal information, or give them advice where deemed

[22] Korokoku no 357 issued on 14 May 2012.

necessary (Arts. 32 and 33). They may recommend that these companies cease or correct any violation of the above regulations (Art. 34, Para. 1), and order them to take the recommended measures immediately cases that involve an imminent risk of serious infringement on the rights or interests of individuals (Para. 2). In an urgent case, orders may be issued without any prior recommendation (Para. 3). Companies violating such orders shall be sentenced to imprisonment with labour of not more than 6 months, or to a fine of not more than 300,000 yen (approximately USD$3,000) (Art. 56). Those that have failed to report or have made false reports concerning Article 32 shall be sentenced to a fine of not more than 300,000 yen (Art. 57). However, no orders or criminal sanctions have been issued to date. Even reports or recommendations are rarely made.[23] This may be because the Ministers have not had the authority to enter private companies, and with limited human resources, violations may be difficult to discover. Also, the required safety measures of the Act are not clear. Orders may not be issued immediately; they may be only issued if the party has not complied with the recommendations.[24]

Concerning civil remedies, Article 25 of the Act, which obliges businesses to disclose any retained personal data to the person concerned upon request, has not been interpreted to provide a basis for a person's claim for disclosure of that personal information (infra 5. d.).[25] This Act is aimed at the prevention of violations of individuals' rights involving privacy. In cases of actual violations, the rights or interests will be restored under the tort provisions mentioned above.[26]

As far as the interpretation of the law of tort is concerned, the principles contained in the Act, in effect, have been seen in courts' decisions (supra 2. a.). Looking at cases, not only confidential matters, but also information about personal identity (name, address, etc.) have been regarded as matters under legal protections. Additionally, not only the acquisition or publication of personal information, but the storing or disclosure of information is also covered as acts potentially invading a person's privacy. It constitutes a tort to fail to take appropriate safeguards for the prevention of information leakage.

For instance, in the case where a company trade union acquired and stored personal information of the company's employees without their consent, the court regarded such an act as tort and they were ordered to pay 210,000 yen (about USD $2,100) as compensation.[27] Regarding information such as the names that were collected officially by the company's trade unions, the acquisition of information was not considered unlawful, but the union's failure to take precautionary measures was considered unlawful (e.g., they did not have passwords on their computers. It was found to be unlawful, because in this particular case, subsequently, the information was leaked to the media. Regarding information, including employees' medical history, religion, political beliefs, etc., which

[23] Following the implementation of the Act, 87 reports were made and one recommendation given in 2005. In 2012, only eight reports were made. In this regard, it should be noted that 'authorized personal information protection organizations', private organizations which are authorized by the competent Ministries, also handle complaints concerning personal information. In 2012, 613 of these complaints were reported. Heisei 24 Nendo Kojin Joho Hogo ni Kansuru Horitsu no Seko Jokyo no Gaiyo [Summary of the Implementation of the Act on the Protection of Personal Information in 2012] < http://www.caa.go.jp/plannning/kojin/24-sekou_3.pdf> accessed on 20 June 2014.

[24] Katsuya Uga, *Joho Kokai Kojin Joho Hogo* (Yuhikaku 2013) 10-11.

[25] Tokyo District Court (27 June 2007), 1978 Hanji 27.

[26] Questions & Answers concerning the Act on the Protection of Personal Information < http://www.caa.go.jp/planning/kojin/gimon-kaitou.html> accessed on 20 June 2014.

[27] The JAL Roso Hoka case, Tokyo District Court (28 October 2010) 1017 Rohan 14.

was collected secretly by a trade union, the acquisition itself was regarded an unlawful act as the employees' consent was not inferred from the context, and there was no legitimate purpose for the union to collect the information. As such, both the regulations of the PPIA 2003 and the basic framework (supra 2. a.) were utilized in this decision, in that it was understood that a person's privacy is invaded when there is no consent given, and where there are no companies' interests superior to the employees' disadvantages, and with regard to the PPIA 2003, the failure to take safeguards was also considered a tort.

Regarding the above, proper remedies remain an issue. The amount of compensation depends on the information acquired or disclosed,[28] as we shall later see. Generally speaking, the amount awarded is highest for improper acquisition or disclosure of medical information (1,500,000-3,000,000 yen or USD $15,000-30,000); and that of criminal convictions (100,000-1,000,000 yen or USD $1,000-10,000). In cases of non-sensitive personal information, such as a person's name, address, etc., the amount of compensation is nominal; about 5,000-10,000 yen or 50 US Dollars.

In short, since the PPIA 2003 is not interpreted as a basis for civil remedies, and the regulations do not specifically address employment relations, the legal basis for employees' privacy protection still resides in the law of tort and labour contracts. Civil remedies are limited in cases where non-confidential matters are involved.

3. Purpose of acquisition and utilisation of employees' personal information

As explained above, when companies use a person's personal information, they must specify a purpose for the use (Art. 15, PPIA 2003), and they must not acquire such information by wrongful means (Art. 17). From another perspective, there are various purposes and means for the acquisition and utilisation of personal information in the workplace. In this regard, the PPIA 2003 has no specific regulations as to when such purposes are to be regarded as proper and reasonable, nor as to when such means are regarded as wrongful. Accordingly, these issues should be resolved by considering both the employee's right of privacy and the existing regulations in the field of employment. The relevant regulations to be explored are found in the law on labour contracts, which have been developed on the basis of civil code provisions and codified in part in the Labour Contract Act of 2007.

A. Recruitment

Investigation of the political beliefs of job applicants

In the recruitment process, companies have been allowed to inquire into and investigate personal matters of job applicants. This 'freedom of investigation' has been in practice since the decision of the Supreme Court in the Mitsubishi Jushi Case.[29] The case arose when a company refused to hire a person for a permanent post upon completion of the required probationary period. The reason for the refusal to hire was that the company had discovered the person had not revealed, and in fact had made false statements about involvement in political activities both in a personal statement, and during an interview in

[28] Jun Masuda, 'Meiyo Kison Praivacy no Shingai' in Osamu Saito ed., *Isharyo Santei no Riron* (Gyosei 2010) 133-140.

[29] The Mitsubishi Jushi case, Supreme Court (12 December 1973), 27-11 Minshu 1536.

the recruitment process.

In court, the applicant argued that inquiring into the political beliefs of a job applicant violated provisions of the Constitution. The reasoning was that he should not have been subject to unfavourable treatment on the basis of this withholding of information. Article 14 of the Constitution provides that 'all 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'. Article 19 of the Constitution prescribes that 'freedom of thought and conscience shall not be violated'. The Supreme Court, however, held that these provisions were aimed at protecting the fundamental freedom and equality of individuals from governmental actions, and were not expected to apply directly to relations between private parties.

The Court's decision concluded that inquiring about matters related to the job applicant's political beliefs were not beyond an acceptable limit. Companies are guaranteed the freedom to conduct business and other economic activities on the basis of Article 22 (the freedom to choose an occupation) and Article 29 (the exercise of property rights) of the Constitution. Accordingly, an employer enjoys the freedom to enter into contracts, and they can freely decide which persons they want to employ. Article 3 of the Labour Standards Act of 1947 provides that an employer shall not engage in discriminatory treatment by reason of nationality, belief, or social status of any worker. However, since this Article covers only treatment 'with respect to wages, working hours or other working conditions', it does not regulate the hiring process. Because Article 3 does not extend the freedom of employment to cover the hiring process, the employer can lawfully investigate a job applicant's political activities.[30]

Dismissal for failure to disclose personal information

A company's freedom of investigation does not always mean that it can lawfully dismiss its employee when it discovers that the employee failed to disclose (or made some false statements about) personal information when requested to disclose such information by the employer during the recruitment process. Such dismissals must be based on reasonable grounds.[31] In the Mitsubishi Jushi case, the Supreme Court held that while a business is allowed in the recruitment process to ask a job applicant to make statements about themselves, the lawfulness of refusal to hire an applicant who has concealed the matters upon the completion of a probationary period depended on: (1) whether, how and why the employee had concealed the matter; and (2) what the employee had concealed and

[30] A number of comments critical of this decision have been made by a number of labour lawyers. See Tadashi Hanami, 'Saiyo no Jiyu to Kihonken' in Tokyo Daigaku Rodoho Kenkyukai (ed), *Rodoho no Shomondai* (Keiso Shobo 1974) 129ff; Takafumi Shimoi, 'Keio Daigaku Igakubu Fuzoku Kosei Joshi Gakuin case' [1976] 101 Kikan Rodoho 94 (note); Yuichiro Mizumachi, 'Saiyo no Jiyu' in Kunishige Sumida and others (eds), *Rodoho no Soten* (3rd edn, Yuhikaku 2004) 130-131; Michio Tsuchida, *Rodo Keiyaku Ho* (Yuhikaku, 2008) 176-178; Akira Watanabe, *Rodoho Kogi Jo* (Shinzansha 2009) 488-489; Satoshi Nishitani, *Rodoho* (2nd edn, Nihonhyoronsha 2013) 136; Takashi Araki, *Rodoho* (2nd edn, Yuhikaku 2013) 306; Akira Hamamura, 'The Mitsubishi Jushi case', in Hiroshi Karatsu and others (eds), *Shinpan Rodoho Jyuyo Hanrei wo yomu I* (note, Nihonhyoronsha 2013) 78-79; Kenji Arita, 'Saiyo no Jiyu', in Michio Tsuchida and Ryuichi Yamakawa (eds), *Rodoho no Soten* (Yuhikaku 2014) 47.

[31] Article 16 of the Labour Contract Act stipulates that a dismissal shall, if it lacks objectively reasonable grounds and is not considered appropriate in general social terms, be treated as an abuse of rights and be considered invalid.

whether he/she had been involved in an unlawful act.

For instance, if a job applicant is still on trial during the hiring process, and there is as yet no criminal conviction on his/her record, the applicant is not obligated to declare it at the time of employment.[32] Additionally, if the convictions had already become 'spent'[33] due to the passage of time, the applicant is not obligated to disclose the details in their personal statement. In one case concerning the a dismissal of an employee who had not disclosed his spent convictions for theft and robbery,[34] the court held that if employers were permitted to inquire about spent convictions and subsequently refused to hire those applicants, applicants with spent criminal convictions would be shackled by their history. Such a result would frustrate the very purpose of the system of spent criminal convictions, i.e., to encourage and support the rehabilitation of eligible offenders. In another case, dismissal of an employee who had not revealed the person's true nationality in the recruitment process was invalidated.[35]

However, protection of employees' privacy had still not been explicitly adopted in these court decisions.[36]

Labour administration guidance

The trend has been changing over the last decade. Labour administration has given guidance to businesses instructing them not to collect personal information of job seekers, including (1) matters which may cause discrimination on grounds of race, ethnicity, social status, origin, address on family register, birth place or any other social discrimination, (2) their thoughts or beliefs and (3) trade union membership.[37]

This guidance stems from the following provision: businesses, when collecting, retaining and using personal information of job seekers, must do so within the scope necessary to achieve the purpose of their businesses and retain and use that information within the scope of the purpose of collection; provided, however, that this shall not apply in a case where the job seeker consents or there is any other good cause (the Employment Security Act, Article 5-4). This provision was added in 1999 to protect the personal information of job applicants. If a business violates the above provision, an improvement order may be issued by the labour administration. If it is not obeyed, imprisonment with labour for six months or less, or a fine of less than 300,000 yen (=about USD $3,000) may be imposed.

[32] The Tanken Seiko case, Tokyo High Court (20 February 1991), 592 Rohan 77.

[33] Article 34-2 of the Penal Code provides that when ten years have passed since a person completed a term of imprisonment without labour or a greater punishment or the person had the execution of such punishment remitted without another sentence of a fine or a greater punishment being imposed, the sentence shall cease to have effect. The same shall apply when five years have passed since a person completed the execution of a fine or a lighter punishment or the person had the execution of a fine or a lighter punishment remitted without another sentence of a fine or a greater punishment being imposed.

[34] The Marja Taxi case, Sendai District Court (19 September 1985), 36-4/5 Rominshu 573.

[35] The Hitachi Seisakusho case (19 June 1974), 25-3 Rominshu 277.

[36] Regarding this issue, see Ikuko Sunaoshi, 'Rodo Keiyaku Teiketsu Riko Katei ni okeru Rodosha no Puraibashi Hogo' (2006) 78-4 Horitsu Jiho 61, 63; Hiroko Tokoro, 'the San Sekiyu case' (2007), 219 Kikan Rodo Ho 260, 262ff; Natsuki Kohno, 'Fuzoku Ten deno Kinmu Keiken no Fushinkoku wo riyu tosuru Chokai Kaiko no Yuko Sei' (2014) 1464 Jurist 12.

[37] Rokoku no 141 issued on 17 November 1999.

Blood tests for job applicants

It should be noted that the Court's decision in the Mitsubishi Jushi case was based not only upon the precedence of a company's freedom of business but also on the reasonableness of the investigation into the person's political activities. The Supreme Court held that it was not unreasonable for a company to be concerned as to whether or not that a person's attitudes or prospective activities may hinder the company's management of staff, and thus to conduct an investigation into a worker's character and beliefs prior to making an employment decision is acceptable. According to the Court, labour relations are continuous human relations that demand mutual trust. This is especially true here in Japan where so called lifetime employment is common.

Therefore, the possibility remains that an investigation of a job applicant, when deemed unreasonable, may be unlawful. Such a possibility was recognised in the B Kin-Yu Koko [Financial Corporation] case,[38] where a corporation in the financial sector conducted a blood test on a job applicant without prior notification to the applicant, in order to determine whether the applicant carried the Hepatitis B virus. Under the tort provision of the Civil Code (Art. 709), the Tokyo District Court ordered the company to pay 1,500,000 yen (approximately USD$15,000) as compensation for the psychological damage suffered by the job applicant.

According to the Court, the average person would not want the fact that they are carries of the Hepatitis B virus to be disclosed to others. Therefore, it is a right of privacy to not have such personal facts acquired by others without their consent. On the other hand, companies have the freedom to conduct health screening on job applicants to confirm whether they possess adequate abilities to perform their job duties. It is a type of freedom of investigation that companies enjoy. On the issue of the necessity of a Hepatitis B blood test, the Court noted that the Hepatitis B virus was transmitted only via blood and that people carrying the virus can be effective at work unless the virus causes chronic Hepatitis. Accordingly, after weighing the needs for the protection of personal information against the freedom of investigation on the part of companies, the Court concluded that companies are not allowed to conduct a Hepatitis B blood test on job applicants in the absence of special circumstances. Even in situations where there is a special need for these blood tests, the company must first notify the applicant of the purpose or requirement of the test and obtain the applicant's consent before proceeding with the test. Since a financial sector corporation, like the respondent company, had little need for carrying out this type of blood test on job applicants, and the corporation did not first explain to the applicant the purpose or requirement for the test, and as the company did not obtain prior consent of the applicant, the Court held that the corporation had committed a tort by invading the applicant's privacy.

B. Disciplinary action

According to case law, companies possess the authority to establish and maintain 'enterprise order'. If employees have committed acts in violation of enterprise order, the company may investigate the details to determine whether disciplinary action is necessary.[39] The acquisition of relevant personal information is authorised by law in cases

[38] The B Kin-Yu Koko [Financial Corporation] (Hepatitis B blood test) case, Tokyo District Court (20 June 2003), 854 Rohan 5.

[39] The Fuji Jyukogyo case, Supreme Court (13 December 1977), 31-7 Minshu 1037.

of sexual harassment, for instance. According to Article 11 of the Equal Employment Opportunities between Men and Women Act, employers shall take all necessary measures to ensure that their employees do not suffer sexual harassment in the workplace. To prevent further harassment, disciplinary action against those who committed said harassment, for instance, are thus authorized by law.[40] If the employer has not taken sufficient measures, they may be liable for damages to the employee harmed by the harassment (Arts. 709 and 715). Before taking disciplinary action, the employer is obligated to conduct an investigation into the facts.[41] Consequently, they have a right to collect information about employee conversations, acts, sexual history, etc., that pertain to the offense.

However, there is still a distinction between on-duty and off-duty conduct, and a growing concern about employees' privacy, as has been seen in cases where employers conducted investigations into the political activities of their employees. In the Kansai Denryoku case,[42] the company sent staff to follow their employees after the employees had left the workplace. The company opened the employees' lockers in the workplace to take photos of a political booklet. The Supreme Court held that, considering that there was no potential for disruption of enterprise order in the case, the acts constituted tortious acts that invaded the employees' privacy. In another instance, where a train company manager happened to find an employee's notebook, and made a copy of the notebook, including information about the employee's thoughts and the employee's relationships, and submitted it to the company, it was regarded as an act of tort.[43] The court acknowledged some lawfulness on the part of the manager, since the manager discovered descriptions of deliberate idleness pertaining to the union's strategy; and in such cases, companies have the authority to investigate to restore enterprise order by taking disciplinary action. However, the means of discovery taken in this instance were not regarded as appropriate, as the notebook involved the employee's private matters and the planned idleness would not have caused substantial damage in any event; unlike the hindrance of train service, for example.

C. Effective human resource management including job allocation

In the context of Japan's long-term employment practices, an employee typically undergoes a change of position once or more during the course of their career in the same company. Such job changes often occur in the course of developing an employee's ability or for the proper deployment of the workforce. This applies, in particular, to those who are being groomed to fulfil a managerial position in the future. It has been understood that employers reserve the right to relocate their employees to fill these different job positions unilaterally.[44]

To ensure that roles are filled by appropriate staff, employers conduct annual performance evaluations.[45] Information about each employee's evaluation is held in the personnel division. Japanese companies, like others, ask job applicants about their academic and occupational experience as well[46] and such information is also held by the

[40] Korokoku no 615 issued on 11 October 2006.
[41] Ibid.
[42] The Kansai Denryoku case, Supreme Court (5 September 1995), 680 Rohan 28.
[43] The JR Tokai Osaka Daiichi Sharyo Sho case, Osaka District Court (29 September 2004), 884 Rohan 38.
[44] The Nissan Jidosha case, Supreme Court (7 December 1989), 554 Rohan 6.
[45] Takayasu Yanagiya, 'Jinji Koka Satei' in Michio Tsuchida and Ryuichi Yamakawa (eds) (n 30) 86-87.
[46] They can lawfully dismiss an employee if they find out that the employee made some false statement

company. Although this information constitutes personal information, the reasoning is that employers must have the authority to acquire, store, and use such information in order to properly allocate positions and roles.

More importantly, in companies where the results of evaluations are held in a database, do the employees have the right to view their evaluation results and to correct them if necessary under PPIA (Art. 26)? This needs further examination (infra 5.d.).

D. Transfer of employees

Employers have been encouraged to obtain and use employees' personal information in order to 'care' for their employees.

Under the long-term or lifetime-employment practice common in Japan, employers also typically reserve the right to transfer their employees to other places of work in other parts of the country. However, in cases where intolerable, significant inconvenience is caused to the employee as a result of the transfer, such an order may be regarded as invalid since it can be seen as an abusive exercise of the right.[47] For instance, in a case concerning an employee ordered to transfer from a city in western Japan to another city near Tokyo, the challenging family situation of the employee caused significant inconveniences and the order of transfer was invalidated.[48]

Therefore, under case law, employers are authorised, or even required to collect information about their employees' family circumstances. Employees, on the other hand, may have legitimate concerns about their privacy when providing the employer with such information. Such concerns can be addressed, in part, by allowing employees to withhold personal family information unless an inconvenient transfer is suggested, or other reason necessitates the disclosure.[49] For instance, the court invalidated an order of transfer, although the employee had not informed his employer of the circumstances involving his children's health in advance.[50]

E. Health and safety compliance

In order to care for employees, Japanese employers have been encouraged to use employees' personal information regarding health and medical condition as well. According to established case law, an employer must give all necessary consideration to securing the safety of an employee, including their life, physical health, and the like. This principle is codified in Article 5 of the Labour Contract Act. When an employer has neglected to take such care and this omission has led to work-related diseases or death of an employee, the employer must pay damages in compensation for the suffering of the employee (Arts. 415 and 709 of the Civil Code). For instance, when an employer observed symptoms of depression in an employee and did not reduce the workload for the employee, although the employee was engaged in discretionary work, the employer was ordered by the Supreme Court to compensate for the damages caused by the result of the disease.[51]

---

about these matters. See, for instance, the Tanken Seiko case (n 32); the Gurabasu case, Tokyo District Court (17 December 2004), 889 Rohan 52.

[47] The Toa Paint case, Supreme Court (14 July 1986) 477 Rohan 6.

[48] The Nestle Nippon case, Osaka High Court (14 April 2006), 915 Rohan 60.

[49] Shozo Yamada, 'Koyo Kankei to Rodosha no Puraibashi' in Nihon Rodo Ho Gakkai (ed), *Rodosha no Zinkaku to Byodo* (Yuhikaku 2000) 71.

[50] The Hokkaido Coca Cola Bottling case, Sapporo District Court (23 July 1997), 723 Rohan 62.

[51] The Dentsu case, Supreme Court (24 March 2000), 54-3 Minshu 1155.

The Industrial Safety and Health Act also imposes the duty on employers to arrange annual medical check-ups for employees (Art. 66). The screenings should include height, weight, eyesight, hearing, thoracic X-ray examination, blood pressure, levels of blood lipid, blood sugar, urine analysis, etc. (Ordinance of Industrial Safety and Health, Art. 44). Employees must undergo these check-ups, and while they may choose to have their medical check-up performed by a physician of their own choice, they must submit the results of the check-up to the employer (the Industrial Safety and Health Act, Art. 66, Para. 5). Employee assistance meetings must also be held for any employees who accumulate more than one hundred or more hours a month in overtime if they request it (Industrial Safety and Health Act, Art. 66-8 and Ordinance on Industrial Safety and Health, Article 52-3).

On the other hand, we should note that there are some restrictions on the acquisition and utilization of employees' information regarding their medical condition. First, 'employee assistance meetings' must be held 'at the request of employees.' Also, certain medical information is considered private and unavailable. In a case where an HIV test was conducted without the consent of the employee, the company was ordered to pay 2,000,000 yen (USD$20,000) to the employee for invading the employee's privacy.[52] According to the court, information about a person's HIV status should be protected as personal information, as it may attract unwarranted prejudice against the person. Furthermore, as the court noted, the virus is transmitted via blood, so infection is highly unlikely in the workplace. As the virus has a long incubation period, the employee can usually continue working without any decrease in job performance. Accordingly, it was held that employers are not allowed to conduct HIV tests on their employees unless specific circumstances apply. The court outlined some of the circumstances that could warrant HIV tests on employees. The court stated that for an HIV test to be justified, the blood test should be reasonably and objectively necessary for maintaining industrial safety and health or for measuring the employee's abilities or aptitude for work. Additionally, the consent of the employee must be obtained after the employee is provided with an explanation of the test and its purpose and necessity. Only when these conditions are satisfied can an HIV test be carried out.

Second, the issue of whether first-hand medical information can be processed by those not in the medical profession has been discussed. According to the Guidelines issued by the Ministry of Health, Labour, and Welfare in 2012, it would be desirable if full information about an employee's disease, such as the name of the disease, be utilized only by an industrial physician or others engaged in occupational health and safety. Ordinary employees should not know about other employee's physical or mental conditions outside of the scope necessary to achieve the purpose.[53] Such a practice would correspond to the businesses' duties concerning security control measures and supervision of employees imposed by PPIA 2003 (Arts. 20 and 21).[54]

[52] The T Kogyo HIV Dismissal case, Chiba District Court (12 June 2000), 785 Rohan 10.
[53] Kihatsu 0611 no 1 issued on on 11 June 2012.
[54] Apart from this, it should be noted that the Industrial Safety and Health Act provides that employees engaged in the implementation of health check-ups owe a duty to keep secret what they have become privy to in the course of doing the check-ups (Art. 104).

4. Personal information protection in the hiring process

The standard for protecting employees' personal information is tied to the stage of employment (see also infra 5. And 6.). Those who seek employment are the least protected. According to the Labour Standards Act, discrimination based on a worker's nationality, social status, or beliefs is prohibited. However, in the Mitsubishi Jushi case, the Supreme Court held that discrimination in the hiring process was not prohibited under this provision (supra 3. a.). This resulted in the acknowledgement of a company's freedom to investigate the applicant's political activities. The Supreme Court, in 2003, expanded the company's freedom of contract to allow an applicant's union membership as a basis of unfavourable treatment in the course of the recruitment process; such treatment is not deemed to be unlawful under Article 7 of the Trade Union Act, which prohibits unfair labour practices.[55]

Japanese employment discrimination law prohibits sex or age discrimination during the hiring process (Equal Employment Opportunities Act, Art. 5 and Employment Measure Act, Art. 10). In 2007, Japan signed the UN Convention on the Rights of Persons with Disabilities Treaty. Subsequently, the Act on Employment Promotion of Persons with Disabilities was amended (in June 2013) to introduce anti-discrimination provisions. These include equal treatment with regard to recruitment and employment (Art. 34). The amended Act will come into force from April 2016.

Even under the existing anti-discrimination legislation, however, no provisions ban the requesting or obtaining of information about an applicant's gender, age, or disability.

Still, reflecting the growing public concern about employees' privacy, the trend is on the side of the employees. Companies must not obtain sensitive medical information about employees or prospective employees, such as HIV status or Hepatitis B test results, unless there are special, justifiable reasons and prior consent has been obtained from the applicant. This interpretation stems from the right to privacy (supra 3. a.).

5. Personal information and privacy protection in employment relations

Those who entered into employment relations are given more protection than job applicants. Additionally, the point of discussion falls more on the appropriateness of the means of collection, the security of information, and the right to control the information.

A. Conditions for obtaining employees' personal information

Regarding the acquisition of personal information, the PPIA 2003 states that the 'means' must not be wrongful. However, 'wrongful means' remains undefined. Since some of the relevant issues have already been mentioned above (supra 2. and 3.), the monitoring of employees, which may be associated with the risk of human rights violations, will be discussed here.

Investigation of criminal acts

[55] The JR Hokkaido Nihon Kamotsu Tetsudo [Kokuro] case, Supreme Court (22 December 2003), 57-11 Minshu 2335. This decision also drew critical comments from labour lawyers. See Kazuo Sugeno, *Rodoho* (10th edn, Kobundo 2012) 770; Satoshi Nishitani, *Rodo Kumiai Ho* (3rd edn, Yuhikaku 2012) 166-167; Takashi Araki, *Rodoho* (2nd edn, Yuhikaku 2013) 641.

The discussion will now focus on investigations into an employee's criminal acts in the workplace. In the Nishinihon Tetsudo case, where a transportation company dismissed their train driver who refused to submit his shoes for a check at the end of the day's operation, the Supreme Court examined the issue of whether the employee have been permitted to disobey the employer's order. In its ruling, the Court set a precedent regarding an employer's inspection of an employee's personal belongings.[56] The Court established this standard after considering the risk of fundamental human rights being violated. The ruling held that such inspections should be based on reasonable grounds; that inspection should be conducted uniformly on all employees in the workplace and as a policy in a generally appropriate manner; and in such a case, an employer does not have to show that there was no alternative means.

The Supreme Court found that in this case the company had carried out the inspection with reference to work rules concerning the illegal concealment of train or bus fares. The Court found that the inspector had been instructed not to inspect employees intrusively or in a provocative manner, and in fact, had made an effort not to do so when inspecting the employee concerned. Accordingly, the manner and extent of inspection was not deemed to be inappropriate. The Court affirmed the legality of the dismissal.

B. Surveillance with electronic devices

There are further limitations using electronic devices to monitor employees. In a case where regular, secret monitoring was carried out, the crucial point was that the employers did not notify the employees of the recording, nor did they obtain prior consent. Another factor was the involvement of employees. The first published case was of the recording and interception of conversations at a workplace. In the case, a train company set up a wiretap on the ceiling of the company waiting room to gather information about the trade union's activities. The court held that the company invaded the employees' privacy. The conversations were held in private and there was no expectation of being overheard.[57] In another case, a driving license school put a recorder into the instructor's automobile and surreptitiously recorded conversations without consent to check on the quality of the lessons. The court held that the school should have explained the reasons for recording, and should have consulted with employees about the manner of implementation, but they did not.[58] These decisions should be supported considering that the ILO Code of Practice also provides that employees should be informed in advance and that the employer should minimize the intrusion on the workers' privacy; and further, before the introduction of any electronic monitoring, the workers' representatives should be informed and consulted (supra 2. b.).

On the other hand, prior notification has not been required in all cases. In cases of ad-hoc email or computer monitoring, a balance test is taken. In a case where an employee mistakenly sent the boss an email critical of him and following this event the boss started monitoring the employee's emails, the court held that the extent of protection of privacy is reduced in cases involving email compared with cases involving phone calls, and her excessive private use of the computer led to such monitoring. Following such an evaluation, weighing the employee's disadvantages against the purposes, processes and manners of the

[56] The Nishinihon Tetsudo case, Supreme Court (2 August 1968), 22-8 Minshu 1603.
[57] The Okayama Denki Kido case, Okayama District Court (17 December 1991), 606 Rohan 50.
[58] The Hirosawa Jidosha Gakko case, Tokuyama District Court (17 November 1986), 488 Rohan 46.

supervisor's actions, it was, in this instance not considered to be a violation of tort law (Art. 709).[59] Considering that the employee exchanged several private emails, and that the boss monitored the emails with another employee after some time had passed, the court held that the employee's privacy was not unlawfully intruded upon. In another case involving private email,[60] it was held that the need for investigation outweighed the need for personal privacy since a reasonable suspicion of slander against another employee had fallen on the employee. They did not notify the employee in advance, since prior notification might have adversely affected the investigation. In addition, the emails were on the company's server (the company's property), therefore, it was not considered inappropriate. The ILO Code of Practice also acknowledges exceptional cases where there is a reasonable suspicion of criminal activity or other serious wrongdoing.

C. Disclosure of a disciplined employee's name or other work-related information within the firm

Companies sometimes take disciplinary actions against employees for the purpose of restoring 'enterprise order' and to prevent a reoccurrence of the same type of misconduct or other unwanted behaviour. Some companies consider disciplinary action to be more effective in association with company-wide announcements. These announcements may detail the type of disciplinary action taken against acts committed by disciplined employees. In contrast, such announcements can be viewed as invading the disciplined employee's privacy and the privacy of any others concerned. In light of the general standards for addressing privacy issues, the means should be within the limits necessary to achieve the purpose. To date, there has been no case law established or academic theory on this point.

However, an examination of the policy on the internal publicizing of disciplinary action carried out against national government employees may provide some guidance on the issue. The policy was introduced in 2003 by the National Personnel Authority.[61] The policy states that:

> (1) The disciplinary actions are announced either when they are related to acts committed in the course of, or in connection with, employment; or, in cases which are not connected with employment, but dismissals or suspensions are taken. (2) The matters to be announced are only the outlines of incidents, the types and dates of disciplinary actions, and the attributes of the employee, such as the employee's department and job position. They should not enable identification of any individual in principle. (3) Some of the above details may be excluded from the announced matters, in cases where such announcements are not regarded as appropriate, for instance, when there is a risk of invasion of privacy of the employee or others concerned. (4) The announcement should be made without delay. Minor incidents may be announced at intervals over a certain period of time. (5) Such announcements may be made by providing a press club with relevant information.

Although there is an inherent difference in the operating environments of the public

[59] The F Sha Establishment (electronic mail) case, Tokyo District Court (3 December 2001), 826 Rohan 46.
[60] The Nikkei Quick Joho case, Tokyo District Court (26 February 2002), 825 Rohan 50.
[61] Jinji-in Jimusocho, Chokai Shobun no Kohyo Shishin ni tsuite, 10 November 2003.

and private sectors, some of the same considerations can be applied across sectors. For example, it is not always necessary to identify a disciplined employee in order to prevent a recurrence of similar incidents or to deter other employees from similar conduct.

D. Employees' right to access, confirm, and request the correction of personal information

As previously explained (supra 2. c.), the employee who is the subject of the data may request and the company must disclose any 'retained personal data'. They must also timely correct any such 'retained personal data' (Art. 26).

An issue has been raised as to whether a data subject should be able to claim in court for the disclosure of such personal data. This issue is connected with the more general question of whether the PPIA 2003 should be regarded as more than a regulatory instrument for governmental control. Or is its purpose to realise a citizen's right of privacy or their right to control their own personal information?

In one case, a patient submitted a request to a hospital to see his/her own charts. After three months, the hospital informed the patient of its refusal to disclose the information requested. The Tokyo District Court held that Article 25 of the PPIA 2003 does not confer data subjects the right of disclosure, and subjects may not make a claim in court for the disclosure of their 'retained personal data' through the courts (see supra 2. c.). According to the Court, the Act expects voluntary resolution of disputes by the companies concerned. The Court suggested that PPIA 2003 clearly provides a mechanism for involvement by competent Ministers in cases where such self-resolutions are not expected to be successful (supra 2.c.).

Some lawyers criticise this approach, because discussion in the legislature seems to be supportive of personal claims.[62]

6. Personal information and privacy protection after the cessation of employment relations

Employees, who are terminated for whatever reason, are given the most protection under the current laws. According to the Labour Standards Act of 1947, when an employee, on the occasion of termination of employment, requests a certificate of employment, the employer is obligated to deliver the certificate without delay (Art. 22, Para. 1 and 2). This certificate may state the period of employment, the occupation, the position of the employee, and/or the reason for termination. If the reason for termination is that the employee was dismissed, the certificate may include the grounds for dismissal. According to the Act, any item that the employee does not request must not be included in the certificate (Para. 3). This specific provision is aimed at protecting employees' privacy.[63] In the certificate, some kind of secret sign must not be included (Para. 4). In addition, information concerning an employee's nationality, creed, social status, or union activities

[62] For more information on this issue, please refer to Tatsuo Ninoseki, 'Kojin Joho Hogo Ho ni motoduku Kaiji Seikyu no Kenrisei', (2008) 59-4 Jiyu to Seigi 140; Masatomo Suzuki, 'Kojin Joho Hogo Ho to Privacy no Kenri,' in Masao Horibe (ed), *Privacy Kojin Joho Hogo no Shin Kadai* (Shoji Homu 2010) 61; Katsuya Uga, *Joho Kokai Kojin Hoho Hogo* (n 24) 324.

[63] Tokyo Daigaku Rodo Ho Kenkyu Kai (ed), *Chushaku Rodo Kijun Ho Jo Kan* (Yuhikaku 2003) [written by Hideyuki Morito] 367.

must not be sent out as part of a premeditated plan with a third party with the intent to impede any other employment prospects of the employee (Art. 4). An employer who violates Paragraph 4 of Article 22 may be sentenced to a term of imprisonment of no more than 6 months, with labour. Alternatively, they may be fined up to 300,000 yen (about USD$ 3,000) (Art. 119). Sanctions that can be applied against violations of Paragraphs 3 are fines of not more than 300,000 yen (about USD$ 3,000) (Art. 120).

According to the government's interpretation, the above list of prohibited communications are exclusive.[64] On the other hand, as long as the personal information of former employees constitutes a database, blacklisting would violate the PPIA 2003, which prohibits employers from providing third parties personal employee information without obtaining the prior consent of the employee (Art. 23). Employers must not provide prospective employers with the personal information of former employees unless it is explicitly authorised by law.

In this regard, it should also be noted that fee-charging employment placement agencies and their employees are prohibited from divulging any personal secrets learned in the course of such businesses or employment (the 1999 Amendment of the Employment Security Act, Art. 51, Para. 1). Fee-charging or non-fee-charging employment placement business providers or their employees, shall not, in any unauthorised way, inform anyone else of any personal information learned concerning his/her work (Art. 51, Para. 2 and Art. 51-2). The same applies to temporary agencies. Such business operators shall not disclose to other persons any secrets learned with regard to matters they handle in the course of business, unless there are justifiable grounds (the 1999 Amendment of the Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers, Art. 24-4).

7. Conclusion

In Japan, an employee's privacy and personal information are protected through a patchwork of case law and statutory regulations. The basic framework emerging from the development of these laws is, at its core, a test of proportionality.

According to this test of proportionality, the lawfulness of the acquisition, utilisation, or disclosure of personal information depends on (1) whether or not the purpose(s) for the use and application of such information is legitimate. From what we have learned, privacy is intruded upon in cases where no legitimate purpose exists (supra 2. c.). Among these purposes, 'the intent to impede the employment of an employee' is the only the purpose which is categorically regarded as illegitimate (Art. 22 of the Labour Standards Act; supra 6.). The regulation of this type of activity is all the more vital when one considers that it may exclude employees not only from employment at a particular company, but also from the labour market as a whole. This can be seen in the governing regulations of employment placement services (supra 6.). Note that, apart from these negative cases, a broad range of purposes are considered legitimate, including recruitment, disciplinary actions, job allocation, transfers, and health and safety (supra 3.).

Thus, in most cases, the lawfulness of an act that potentially intrudes upon an employee's privacy depends on (2) how disadvantageous the acquisition or disclosure of the personal information is, or how confidential that information may be. However, it also

[64] Kihatsu no 502 issued on 15 December 1947.

depends on (3) the extent to which the acquisition or disclosure of personal information is necessary to achieve a purpose, and (4) whether the employer has used appropriate means to obtain the information. The results of such decisions are guided by balancing the disadvantages of employees against the necessity of employers. The appropriateness of the means is also considered in this balance.

(2) The courts evaluate how disadvantageous the confidential information can be to the employees. Sensitive medical information has been given maximum protection. Concerning the acquisition of information about whether employees are carriers of HIV virus or the Hepatitis B virus, case law requires the existence of special circumstances (necessity based on employees' abilities to perform job duties) and employees' prior consent (supra 3. a. and 3. e.). The second most important protection is reserved for employees' political activities. Collecting information about workers' political activities is regarded as an invasion of privacy in the course of employment (unless it is relevant to 'enterprise order'; supra 3. b.), while such collection in the hiring process is not regarded as an illegal act (supra 3. a.). This is based on the idea that, in the hiring process, it is not unreasonable for a company to have concerns about job applicants' prospective actions and attitudes. In this way, (3) with this necessity in mind, the balance is tilted toward the companies in such cases. This argument was strengthened by reference to the special character of employment relations, as human relations require mutual trust, with respect to the long term employment practices of Japan. Similarly, for the purpose of preventing sexual harassment in the workplace, employers may ask employees about their experiences of sexual harassment (supra 3. b.). In order to ensure the health of employees, employers are even required, by law, to acquire and utilize medical information about employees (supra 3. e.) as long as it does not involve overly sensitive information. The same applies to inquiries into an employee's family life (3. d.). Thus, confidential information may be collected by employers, depending on the reason and extent of the necessity and purpose.

(3) On the other hand, an examination of this necessity may lead to the decision that employers' acts are unnecessary to achieve their purpose and are considered unlawful in that they have intruded upon an employee's privacy. Following employees to investigate their political activities is considered unlawful (supra 3. b.). In addition, a statutory regulation (the PPIA 2003) requires the employer to specify the purposes for which personal information is to be used (Art. 15). The employer is not allowed to process personal information beyond the parameters necessary for the fulfilment of these specified purposes, without the prior consent of the employee (Art. 16).

(4) The appropriateness, of the manner of acquisition of personal information has been examined by the courts, as evidenced by cases of investigation into criminal acts (supra 5. a.). According to the case law, a company needs to have an established policy for the investigation of criminal acts and the manner of investigation should not be intrusive. In cases of regular monitoring with electronic devices, prior notification is needed, and the involvement of trade unions should be taken into consideration (supra 5. b.).

Such a general framework seems to be suitable for issues of privacy and personal information. The same, unified rules cannot be applied to all cases involving such issues, since the extent of the company's necessity and disadvantages to the employees are different, depending on the matters involved and the context. The laws also need to be flexible in order to take into account both parties' interests, but must do so in light of societies' growing concern for the protection of privacy. In fact, recent case law has shown this to be true (supra 3. a. and 3. b.).

A possible limitation of such a balancing test may be that, in the case of personal information which is not confidential, protection might not be given. However, the scope of the PPIA 2003 has already been extended to personally identifiable information and includes regulations on safeguards of all personal data. Recent court decisions on breaches of non-confidential information have acknowledged them as torts under the provisions of the Civil Code (supra 2. c.). Thus, the scope of protection is already expanding in this respect.

Furthermore, the narrow framing of sensitive data as a reflection of freedom of contract and freedom of investigation should be examined. There has not been protective regulation concerning the acquisition of sensitive data such as employees' political, religious or other beliefs, especially in the hiring process (supra 3. a., 3. b., and 4.). Considering that certain matters are subject to specific protection under the ILO Code of Practice (supra 2. b.), Japan should re-examine whether its regulations do the same. In particular, since life-time employment practices are not as prevalent as they were, the necessity of obtaining a significant amount of personal information may now not be needed at as many workplaces as in the past.

In addition, with regard to personal information which an employer acquires in order to care for their employees, such as health or family background, security control measures should be strengthened. One example is an interpretation of the PPIA 2003 issued recently concerning the processing of medical data. According to the current interpretation, the desirable practice is that full information, such as the employee's diagnoses, be utilized only by industrial physicians and other authorised parties, etc. (supra 3. e.). Moreover, such personal information should only be provided by employees if they are seeking special accommodation from the employer (supra 3. e.).

In this regard, special consideration should be given to the character of employment relations. For instance, along with a proportionality test, the Supreme Court has taken into consideration the consent of concerned parties, when deciding whether an invasion of privacy was justified (supra 2. a.). In the employment field, by contrast, we should keep in mind that the ILO Code of Practice sets a certain standard regarding the consent of employees about their privacy (supra 2. b.). This point should be the subject of further discussion and examination.

An additional area of interest is how the PPIA 2003 effectively limits its scope to employers or workplaces that have at least 5,000 people[65] and how the Act does not provide for civil remedies, in particular, in the context of disclosure of personal information (supra 5. d.). 'The right to control one's own information' has yet to be confirmed. Whether maintaining such limitations is appropriate or not will be discussed further at a later date.

[65] Uga argues that the range of application of the Act should be gradually extended to small-and-medium-sized businesses. Uga, *Kozin Joho Hogo no Riron to Jitsumu* (n 21) 72.